Chapter 6

Criminal penalties for procuring confidential information

This chapter deals with the criminal penalties which apply to those who procure the wrongful disclosure of third party information. Procuring confidential information involves enticing public servants to unlawfully disclose information. This conduct is not expressly prohibited in all statutes. However, some statutes contain provisions which do expressly prohibit procuring or soliciting protected information and some examples of those provisions are outlined. The Committee concludes that there is a need for reform in this area to ensure that the procuring of confidential information is prohibited in all circumstances.

6.1 Introduction

6.1.1 This section focuses on the adequacy of the existing criminal penalties which can be applied in relation to persons who procure the wrongful disclosure of third party information. The general sentencing provisions in the Crimes Act outlined at paragraph 5.4.3 are also relevant in this context.

6.1.2 In recent years there has been increasing recognition of the number of cases where the wrongful disclosure of confidential third party information is procured from Commonwealth agencies. Procuring information involves enticing public servants to leak information to, for example, inquiry agents who may then sell this information to financial institutions so that those institutions can locate debtors.[360] The Privacy Commissioner has commented on procuring the disclosure of confidential information. He has stated that:

> The ultimate responsibility for wiping out the practice of bribing public servants lies with those who engage the private investigators - banks, finance companies, insurance companies and the like. While they may see their needs - to locate defaulters for example – as justifying whatever steps are being taken to obtain relevant information, they should reconsider that attitude. By turning a blind eye to private investigators' activities, and paying well for the service rendered, they are creating an environment of disregard for the confidentiality of information held by government agencies.[361]

6.1.3 The DPP identified some general problems in prosecuting persons who have procured the wrongful disclosure of information. The prosecution must show that the information was obtained from a Commonwealth agency and not some other source. It

---

360 Attorney-General's Department, *Submissions*, p. S391.

361 *Second Annual Report on the Operation of the Privacy Act*, op. cit., p.16 cited in Attorney-General's Department, *Submissions*, p. S392.

must also show that the person did not come by the information innocently. Furthermore, the prosecution must be able to negate the possibility that the defendant was sent the confidential information anonymously and it must also negate the possibility that the information was obtained from an intermediary (who may have been the person that actually induced the Commonwealth officer to disclose the information).[362]

6.2 Provisions relevant to procurement

6.2.1 There is no general provision in the Crimes Act which makes it an offence for a person to procure the wrongful disclosure of third party information from a Commonwealth officer. However, certain sections of the Crimes Act are relevant to this issue.

6.2.2 Section 70 of the Crimes Act does not directly apply to secondary disclosures. However, subsection 5(1) provides that:

> Any person who aids, abets, counsels, or procures, or by act or omission is in any way directly or indirectly knowingly concerned in, or party to the commission of any offence against any law of the Commonwealth or of a Territory . . . shall be deemed to have committed an offence and shall be punishable accordingly.

Subsection 5(1) would facilitate the prosecution of a person who came to an arrangement with a Commonwealth officer for that officer to unlawfully disclose information to that person. Evidently the aider/abettor is liable to the same maximum penalty as the principal offender.

6.2.3 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 under section 70 of the Crimes Act as the aiding and abetting provisions would not apply.[363]

6.2.4 Section 7A of the Crimes Act, which deals with the incitement of offences against Commonwealth law, is also relevant in this context. It provides that:

---

362 *Submissions*, p. S31.

363 See Attorney-General's Department, *Submissions*, p. S393. Subsection 79(3) may extend to third parties, but it would have to be demonstrated that the third party had a duty not to disclose the information. (See Attorney-General's Department, *Submissions*, p. S360).

> If any person:
> (a) incites to, urges, aids or encourages; or
> (b) prints or publishes any writing which incites to, urges, aids or encourages;
> the commission of offences against any law of the Commonwealth or the carrying on of any operations for or by the commission of such offences, he shall be guilty of an offence.

The maximum penalty for an offence under section 7A is the same as the maximum penalty for the principal offence.

6.2.5 The ATO noted that section 86 of the Crimes Act may also be relevant in this context.[364] Section 86 deals with conspiring to commit Commonwealth offences. The maximum penalty is three years imprisonment[365] or if the conspiracy involved the commission of a Commonwealth offence punishable by more than three years imprisonment, the penalty is the same as for the principal offence[366]. Section 86 will be repealed by the *Crimes Amendment Act 1995* which has not yet been proclaimed.[367] The new section 86(1) provides that if a person conspires to commit a Commonwealth offence punishable by more than 12 months imprisonment or by a fine of 200 penalty units or more, then that person is guilty of the offence of conspiracy to commit the offence. The offender is punishable as if the offence to which the conspiracy relates had been committed. The amendments require an overt act on the part of one of the parties to the agreement which forms the conspiracy and proceedings can only be commenced with the consent of the DPP.[368]

6.2.6 Under the terms of reference, the Committee must consider the penalties relevant to those who procure the wrongful disclosure of third party information. When discussing this term of reference, a number of submissions tended to refer to the provisions dealing with soliciting the disclosure of third party information in the specific statutes.[369] It is unclear whether there is a difference in meaning between 'procuring' and 'soliciting'. Procuring means 'to acquire or obtain'[370] while soliciting has been defined as 'to ask

---

364 *Submissions*, p. S334.

365 See paragraph 86(2)(a) of the Crimes Act.

366 Paragraph 86(2)(b) of the Crimes Act.

367 The Act was assented to on 15 March 1995 but it had not been proclaimed as at 23 June 1995.

368 See Second Reading Speech by the Hon Duncan Kerr MP, Minister for Justice, House of Representatives *Hansard* 1 March 1995, p. 1336 and see also new subsections 86(3) and 86(9) of the Crimes Act (as amended by the Crimes Amendment Act).

369 See, for example, Attorney-General's Department, *Submissions*, p. S393.

370 See Nolan J. and Nolan-Haley J., *Black's Law Dictionary*, sixth edition, West Publishing Co., St Paul, Minn., 1990, pp. 1208 and *Stroud's Judicial Dictionary*, fifth edition, Sweet & Maxwell Ltd, London, 1986, pp. 2038-2039.

for the purpose of receiving, to appeal, to try to obtain'[371]. 'Solicit' is defined in the Privacy Act as:

> in relation to personal information, to request a person to provide that information, or a kind of information in which that information is included.[372]

None of the submissions commented on a possible distinction between the terms.

6.2.7 Some departments have specific provisions which deal with soliciting/procuring third party information. For example, the *Taxation Administration Act 1953* provides that a person must not knowingly take action for the purpose of obtaining information about another person's taxation affairs[373]. The maximum penalty for this offence is $10 000 or 2 years imprisonment or both.

6.2.8 The *Social Security Act 1991* prohibits a person from intentionally obtaining information where the person knows or ought reasonably to know that the information is protected.[374] The Act also prohibits soliciting the disclosure of protected information from an officer or another person where the person soliciting knows or ought reasonably to know that the information is protected.[375] The Act specifies that an offence is committed whether or not any protected information is actually disclosed. This would enable those who 'fish' for third party information, which they believe may be held by the Department, to be prosecuted.[376] The maximum penalty for soliciting protected information from DSS is two years imprisonment.

6.2.9 It is interesting to note that the definition of 'protected information' in the Social Security Act was recently amended[377] to ensure that the confidentiality provisions protect the information that a person *is not* a client of the Department. This is particularly relevant in relation to soliciting. The Explanatory Memorandum notes that when the Department is approached by a person soliciting information, it is not uncommon for information to be solicited about a person who is thought to be a client, but is in fact unknown to the Department.[378]

---

371 *Black's Law Dictionary*, op. cit., p. 1392.

372 See subsection 6(1) of the Privacy Act.

373 See section 8XA of the Taxation Administration Act.

374 Section 1312A of the Social Security Act.

375 Section 1316 of the Social Security Act.

376 See comment in *Submissions*, pp. S441–S442 before amendments to the Act were made.

377 Section 12 of the *Social Security Legislation Amendment Act 1994* (No. 63, 1994).

378 p. 17 of the Explanatory Memorandum.

6.2.10 It is also an offence under the Social Security Act to solicit the disclosure of protected information and with that purpose in mind, make a representation which the person knows or ought reasonably know is untrue.[379] An offence is committed regardless of whether any protected information is actually disclosed. The maximum penalty for this offence is two years imprisonment.

6.2.11 The Health Insurance Act and the National Health Act also prohibit soliciting the disclosure of protected information. The soliciting provisions in those acts are substantially the same as those in the Social Security Act.[380] The Acts also provide that when protected information is disclosed, the person is guilty of an offence if he or she knows or ought reasonably know that the disclosure was unlawful and he or she either solicited the information, disclosed the information to another person or used the information otherwise than by disclosing it to another person.[381] The penalty for these offences under both statutes is two years imprisonment, which means that the maximum penalties for soliciting offences under the Social Security Act, the Health Insurance Act and the National Health Act are all consistent.

6.3 Adequacy of applicable penalties

6.3.1 Proving that confidential information has been procured in contravention of the Crimes Act may be problematic. As outlined previously, subsection 5(1) of the Crimes Act does not cover the situation where a person is the second or later recipient of unlawfully disclosed information, but had no direct or indirect involvement in the commission of the original offence by the Commonwealth officer. A specific offence would need to be created to cover such cases.[382] The Attorney-General's Department noted that similar problems are associated with the application of the corruption and bribery offence in subsection 73(2) of the Crimes Act.[383]

6.3.2 The Department of Employment Education and Training (DEET) commented that the existing penalties in relation to procurement are inadequate and suggested that the Crimes Act provisions in this area should be strengthened.[384]

---

379 Section 1316A of the Social Security Act.

380 Subsection 130(14) of the Health Insurance Act, subsection 135A(13) of the National Health Act.

381 Subsection 130(15) of the Health Insurance Act and subsection 135A(14) of the National Health Act.

382 Attorney-General's Department, *Submissions*, p. S393.

383 ibid.

384 *Submissions*, p. S930.

6.3.3 Some submissions suggested that existing penalties in the specific statutes in relation to procuring the wrongful disclosure of information in the are inadequate. For example, the ACS informed the Committee that little can be done to penalise persons who procure the wrongful disclosure of information under the Customs legislation (unless that person meets the description of persons to whom section 16 of the *Customs Administration Act 1985* applies).[385] However, the ATO submitted that the penalties which attach to procurement offences in the *Income Tax Assessment Act 1936* and the Taxation Administration Act were adequate.[386]

6.3.4 DSS commented that the problem lies not with the adequacy of the penalties, but rather with the difficulties in proving that someone who obtained information indirectly has committed an offence.[387]

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

6.3.6 The Attorney-General's Department 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.[388] Section 8XB of the Taxation Administration Act was cited as a method of dealing with that potential problem. The effect of subsection 8XB(2) is that a person has obtained taxation information in breach of a tax law if:

> (a) the information relates to the affairs of another;
> (b) the circumstances in which the information was obtained would have led a reasonable person to believe that, in the case of information contained in a document, the document had come from the Commissioner or Deputy Commissioner's office or, in any other case, the information had come from the records of the Commissioner or another officer; and
> (c) the information was obtained in circumstances that gave the recipient no reasonable cause to believe that communication of the information was authorised by law.

6.3.7 Evidence was given to the Committee concerning the operation of section 8XB of the Taxation Administration Act. Under that provision, actual disclosure by an ATO

---

385 *Submissions*, p. S494.

386 *Submissions*, pp. S334–S335.

387 DSS, *Submissions*, p. S448.

388 *Submissions*, p. 394.

officer does not have to be proved. It is necessary only to show that the information came from ATO records.[389] The provision places a direct obligation on a person to whom tax information has been improperly released not to further disseminate it.[390] The DPP noted that section 8XB overcomes two potential obstacles for prosecution, namely, that there is no need to prove that the third party was involved in the improper release of the information and there is no need to prove that the information was unlawfully disclosed.[391] The Attorney-General's Department commented that this provision is effective in penalising the principal behind the disclosure (for example, banks and finance companies) and not only the person who initially acquired the information (for example, a private inquiry agent).[392]

6.3.8 According to the DPP, the onus of proof has not been reversed in section 8XB of the Taxation Administration Act. But rather section 8XB places an obligation on a third party to treat as confidential any taxation information in his or her possession which the defendant either knows has been disclosed unlawfully, or which he or she should realise has probably been disclosed unlawfully.[393]

6.3.9 While section 8XB has been discussed in favourable terms as a method of protecting confidential information, the DPP noted that there are still two hurdles to any prosecution under section 8XB of the Taxation Administration Act. First, it is still necessary for the prosecution to show how the defendant came to be in possession of the relevant information and if the third party declines to explain how he or she came to possess the information, it may not be possible to prosecute. Secondly, it remains necessary for the prosecution to show that the information originated from the ATO. The DPP may be assisted in proving that element by section 8XB(2)(b) which provides that it can be assumed the ATO is the source if the form and circumstances in which the information was obtained would have led a reasonable person to believe it came from the ATO. However, the DPP suggests that if it cannot prove how the information came to the defendant, it may have difficulty in showing that the information did not come from a source other than the ATO.[394] The DPP concludes that section 8XB does not

---

389 ibid., p. S394.

390 DPP, *Submissions*, p. S976. Note also that under section 1312B of the Social Security Act dissemination after receipt (that is, recording, disclosing or otherwise using) is an offence.

391 ibid., p. S977.

392 *Submissions*, pp. S394 and S406.

393 DPP, *Submissions*, p. S977.

394 ibid.

resolve all the problems that arise in attempting to protect third party tax information, but it does take steps in the right direction.[395]

6.4 Conclusions

6.4.1 The Committee considers that, in order to adequately protect third party interests, procuring the disclosure of confidential third party information held by the Government should be prohibited in all circumstances. While some agencies have enacted relatively comprehensive provisions in departmental legislation which prohibit procurement, that conduct is not prohibited by specific provisions in all statutes.

6.4.2 Furthermore, there are difficulties in relying on the Crimes Act as subsection 5(1) can only be invoked in limited circumstances and has no application where a second or later recipient of unlawfully disclosed information had no direct or indirect involvement in the commission of the original offence. This means that the Crimes Act will not always cover the field if there are inadequacies in the specific secrecy provisions. As the procurement of confidential third party information is not adequately prohibited in all circumstances, there is a need for reform. Reform proposals are discussed in the next chapter.

395 ibid., pp. S977-978.

Chapter 7

Application and rationalisation of the criminal law

This chapter outlines the Committee's proposals for reform of the criminal law in its protection of confidential information. The chapter begins by examining the situations in which the application of the criminal law may be an appropriate response to the misuse of confidential third party information. It then considers the categories of information which should be protected by the criminal law and the type of provisions which would most adequately protect those categories.

The Committee recommends the insertion of general offence provisions in the Crimes Act. It considers that general provisions will provide a central focus. Placement of those provisions in the Crimes Act indicates the seriousness with which the offences are viewed and may act as a greater deterrent than if the provisions were included in another statute.

The chapter concludes with an examination of the conduct that should be prohibited by the offence provisions. The Committee considers that the Crimes Act should prohibit unauthorised dealing in confidential third party information at every point on the distribution chain.

7.1 Introduction

7.1.1 This chapter deals with the application the criminal law should have in protecting confidential third party information. The Committee then considers the merits of general secrecy provisions protecting third party information (as opposed to retention of the current secrecy provisions scattered throughout various Commonwealth laws) and discusses the most appropriate location for general provisions. The Committee concludes by discussing options for rationalisation of the existing secrecy provisions and the type of conduct that should be prohibited.

7.2 Is the application of the criminal law an appropriate response?

7.2.1 As discussed in chapter 4, secrecy provisions should not be used to regulate the lawful transfer of third party information between government agencies. Secrecy provisions are however relevant in regulating the flow of information from government agencies to the general public. Consequently, the application which the criminal law should have in relation to the protection of confidential personal and commercial information is a fundamental issue.

7.2.2 The AFP submitted that this issue may be addressed by balancing the competing social, rather than legal, considerations. On one hand, there is the view that the application of the criminal law is justified only by the degree of harm to the public interest[396], thus the public interest would need to be severely affected before the criminal law should be invoked. Alternatively, it could be argued that the application of the criminal law in prohibiting some activities has broader implications. It was suggested that:

> . . . criminal law provisions have an attendant reassuring effect; an effect which in some cases may be a necessary element for government activity. When seeking information, there are clear advantages in an ability to refer to a statutory guarantee of confidentiality.[397]

7.2.3 There may be different perceptions as to that which constitutes harm to the public interest. For example, GIO Australia suggested that in its view most individuals would place a higher priority on protecting the community's financial interests than protecting personal privacy.[398]

7.2.4 The AFP suggested that where law enforcement is concerned, there is a public acceptance that the criminal law is an appropriate response to protect third party information.[399] The AFP did note, however, that it may consider alternative methods of protecting information in its organisation. These methods may include the maintenance, extension or introduction of formal and informal sanctions within the AFP career structure, further refinement of security checks and clearance procedures, more intensive and disciplined training for new employees and greater attention to security classifications and documents containing classified material.[400]

7.2.5 The Attorney-General's Department agreed that the application of the criminal law is appropriate to protect third party information. However, the Department submitted that in some instances, alternative remedies may be more appropriate and effective than criminal sanctions. Those remedies include formal disciplinary procedures, informal sanctions within the public service (for example, allocation to less attractive employment),

---

396 *Submissions*, p. S76.

397 ibid.

398 *Submissions*, p. S44.

399 *Submissions*, p. S76.

400 *Submissions*, p. S74.

utilising the law on breach of confidence[401] or seeking a determination under the Privacy Act.[402]

7.2.6 The Attorney-General's Department considered that in some cases alternative remedies are superior to the criminal law in dealing with the unauthorised disclosure of personal information. The advantages of alternative remedies are that:

- some of those measure embody preventative principles which may provide more appropriate redress for third parties;
- the measures are less costly than criminal proceedings; and
- third parties can access remedies without invoking the processes of the criminal law.[403]

7.2.7 It was generally agreed that the unauthorised disclosure and procurement of confidential third party information is an appropriate matter for the criminal law in certain circumstances.[404] Criminal sanctions were considered particularly appropriate where information is deliberately released for profit, or with malicious intent, or possibly where the disclosure is made recklessly.[405]

7.2.8 However, the criminal law should not operate more widely than is needed and it should not be invoked unless there is a specific reason for giving certain information special protection.[406] The reason for restricting the application of the criminal law is that the imposition of criminal sanctions can have serious repercussions and may involve deprivation of liberty. Consequently, penal sanctions should be reserved for serious offences where the public interest is best served by imposing those sanctions on the offender.

7.2.9 While the Department considered that criminal sanctions should continue to apply in relation to the unauthorised disclosure of confidential third party information, it emphasised that prosecution should not be an automatic response.[407] The DPP agreed, noting that not all breaches of secrecy provisions should be dealt with by

---

401 The law on breach of confidence is outlined in chapter 2 and further discussed in chapter 8.

402 *Submissions*, p. S395.

403 ibid, p. S396.

404 For example, DEET, *Submissions*, p. S930.

405 Department of Health, Housing and Community Services, *Submissions*, p. S626.

406 McGuiness, op. cit., p. 72.

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

prosecution.[408] According to the Prosecution Policy of the Commonwealth, criminal charges should only be laid if there is a reasonable prospect of conviction and if the prosecution is in the public interest.[409]

7.2.10 On the other hand, alternative sanctions are not appropriate in all cases. Disciplinary provisions only apply to public servants. Such provisions are inapplicable to private individuals who gain access to Commonwealth third party information, people who have retired from the Public Service and those who resign when investigations commence.[410]

7.2.11 The Committee concludes that the criminal law does have a major role to play in the protection of confidential third party information, although it notes the value of alternative remedies and other measures such as computer audit trails and the development of a privacy culture. The Committee suggests that the imposition of criminal sanctions reflects the seriousness of the crime and the community view of the gravity of the offence. Furthermore, criminal sanctions have a greater deterrent value than alternative remedies.

7.3 The Gibbs Committee and the information that should be protected

7.3.1 The application of the criminal law to the disclosure of information was considered in the Review of Commonwealth Criminal Law. The Committee of the Review (the Gibbs Committee) released its final report in December 1991. The Gibbs Committee recommended that section 70 and subsection 79(3) of the Crimes Act should be repealed and that, in line with the *Official Secrets Act 1989* (UK), the criminal law should only apply to the unauthorised disclosure of a limited number of narrowly described categories of official information which are no broader than that which is required for the effective functioning of Government.[411]

7.3.2 Those categories included information relating to the intelligence and security services, defence, foreign affairs, information obtained in confidence from other governments or international organisations and information where unauthorised

---

408 *Submissions*, p. S1073.

409 See *Prosecution Policy of the Commonwealth: Guidelines for the making of decisions in the prosecution process*, AGPS, Canberra, 1993, pp. 3–6.

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

411 Review of Commonwealth Criminal Law, *Final Report*, AGPS, Canberra, December 1991, pp. 234, 330.

disclosure would be likely to result in the commission of an offence, facilitate an escape from custody or impede the prevention or detection of an offence or the apprehension of an offender.[412] The Gibbs Committee expressly excluded a number of categories of information from the categories of official information on which it focussed. The excluded categories of information that are relevant to this inquiry are information supplied in confidence and information affecting personal privacy.[413] The recommendations of the Gibbs Committee therefore, related to the role of the general criminal law in relation to the disclosure of official, as opposed to third party, information.

7.3.3 If enacted, the recommendations of the Gibbs Committee would reduce the existing protection of third party information offered by the 'umbrella' provisions in section 70 and subsection 79(3) of the Crimes Act[414] because the recommended categories do not include confidential personal or commercial information. The ICAC report went further than the Gibbs Committee in this area by recommending that a policy be developed in respect of all government-held records to determine information to be made available and that to be protected.[415]

7.3.4 The recommendations of the Gibbs Committee are directed towards limiting the protection of the general criminal law to situations where the unauthorised disclosure of information could harm the public interest.[416] The Gibbs Committee thought that unauthorised disclosure of confidential third party information should be prohibited by criminal sanctions in statutes other than the Crimes Act. The Gibbs Committee commented that if there were a general prohibition on the disclosure of information supplied in confidence, it would need to be accompanied by a defence of public interest or iniquity which would be a significant complication. The Gibbs Committee went on to state that:

> Having regard to this and the fact that the basic purpose of the proposed provisions is to protect information the disclosure of which would seriously harm the public interest, the Review Committee considers that the better course is that, while retaining and, if necessary, extending the provisions of special Acts . . . , protection of other forms of information supplied to the Government in confidence (other than that supplied by other governments or international organisations . . .) should not be the subject of a general criminal law.[417]

412 ibid., pp. 330–331.

413 ibid., p. 332.

414 Attorney-General's Department, *Submissions*, p. S375.

415 *ICAC Report*, op. cit., p. 217 cited in ANAO, *Submissions*, p. S143.

416 Attorney-General's Department, *Submissions*, p. S375.

417 *Final Report*, p. 319.

Thus, the Gibbs Committee concluded that the disclosure of confidential personal information should not be the subject of a general criminal law (that is, the Crimes Act), but rather it should be dealt with by specific statutes.

7.4 Views on the recommendations of the Gibbs Committee

7.4.1 The Business Council of Australia supported the view of the Gibbs Committee that it is undesirable to apply the criminal law to all unauthorised disclosures of information. The Business Council suggested that criminal provisions should only be applicable where disclosure seriously harms the 'public interest'.[418] A number of other submissions agreed with the recommendation of the Gibbs Committee.[419]

7.4.2 However, while the Department of Health, Housing and Community Services (as it then was) agreed with the categories of official information recommended for protection in the Crimes Act by the Gibbs Committee, it was concerned that if the Crimes Act were amended in the manner recommended by the Committee, the Department would not be able to rely wholly on the provisions of that Act to protect sensitive information which is not subject to a specific secrecy provision.[420]

7.4.3 The ATO thought that other categories of information should have been included in the categories of information to be protected by the Crimes Act. These additional categories are personal and commercial information and limited categories of policy and administrative information.[421] The ATO suggested that the revelation of confidential departmental information, such as the ATO computer system for identifying audit cases, would undermine the work of the ATO.[422] The Committee views a consideration of the protection which should be afforded to sensitive policy and administrative information as outside the terms of reference of this inquiry.

7.4.4 The ATO noted that if section 70 of the Crimes Act did not apply to the disclosure of confidential personal and commercial information, it would be able to rely on the secrecy provisions in taxation laws. However, the ATO considered that this would not be as effective a deterrent as the Crimes Act because disclosure of information other than

---

418 *Submissions*, p. S240.

419 For example, Department of Health, Housing and Community Services (as it then was), *Submissions*, p. S626 and Department of Industrial Relations, *Submissions*, p. S713.

420 *Submissions*, p. S626.

421 *Submissions*, p. S335 and *Transcript*, p. 298.

422 *Transcript*, p. 298.

personal information concerning taxpayers is not covered by the tax secrecy provisions.[423] Other submissions also appeared to support the inclusion of provisions in the Crimes Act dealing with the unauthorised disclosure of confidential third party information.[424]

7.5 The utility of general provisions

7.5.1 A number of submissions commented on the utility of general prohibitions concerning the unauthorised disclosure of confidential third party information. The Attorney-General's Department appeared to support a general provision or one general constellation of provisions in the Crimes Act.[425] The Privacy Commissioner was also in favour of a general provision dealing with soliciting protected information which would be applicable to all Commonwealth agencies[426] or a systematic system of criminal offence provisions dealing with those that procure the improper disclosure of personal data[427]. The Director of Public Prosecutions agreed that it would be preferable to have a general provision applying across all Commonwealth agencies.[428]

a) Factors in support of general provisions

7.5.2 There are a number of arguments that have been advanced in support of more general provisions dealing with the protection of confidential third party information. General provisions would:

- recognise the need for a rational and consistent approach given the burgeoning number of secrecy provisions;
- underline the overall need for officers to protect confidential third party information[429];
- mean that elements of each offence (particularly the mental element) would be the same and therefore, avoid the problem where officers who disclose information obtained under one enactment may face prosecution while other

423 ibid.

424 See, for example, DEET, *Submissions*, p. S930.

425 *Submissions*, p. S341 (abstract) and p.S393 (para. 7.3.2); *Transcript*, p. 171.

426 *Submissions*, p. S583.

427 *Transcript*, p. 478.

428 *Submissions*, p. S31.

429 Attorney-General's Department, *Submissions*, p. S389.

officers who disclose similar information, obtained under a different enactment, may not be subject to criminal sanctions[430];

- similarly, 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[431];
- ensure that where information is passed from one agency to another, the criminal protection for that information would remain the same[432];
- enable the application of a consistent set of penalties, according to the sensitivity of the information involved[433];
- a uniform law may be easier for investigative and law enforcement bodies to apply (particularly if information has been solicited from a range of government sources)[434];
- a general provision or general provisions would be easier to amend, if it became evident that further refinement was necessary; and
- result in officers across the Public Service becoming familiar with one set of obligations[435].

b) Factors in support of retaining the specific secrecy provisions

7.5.3 There are, however, a number of arguments that can be advanced in support of retaining the specific secrecy provisions. Those arguments include the following:

- as many of the existing provisions are designed to protect information relevant to various statutes (for example, Social Security provisions), the obligations in relation to disclosure should be located in the same legal instrument which sets out the regime for acquiring the information[436];
- most officers are aware of their current obligations and the introduction of a new regime would require re-education[437];
- a single blanket provision aimed at protecting all third party confidential information may lead to increased and unnecessary secrecy in government[438];

---

430 *ibid. See also Director of Public Prosecutions, Submissions, p. S30.*

431 Privacy Commissioner, *Submissions*, p. S583. In this context, the DPP also suggested that the position of people dealing with Commonwealth officers would be clear if there was a general provision which applied to all Commonwealth agencies (*Submissions*, p. S31).

432 Attorney-General's Department, *Submissions*, p. S389.

433 ibid.

434 Privacy Commissioner, *Submissions*, p. S583.

435 Attorney-General's Department, *Submissions*, p. S389.

436 Attorney-General's Department, *Submissions*, p. S388.

437 ibid.

438 ibid.

- the category of protected information would need to be carefully defined to ensure that innocuous disclosures of information did not attract criminal penalties[439];
- a single provision may need considerable qualification to satisfy the specific confidentiality needs of certain agencies (for example, the ATO)[440]; and
- departments may wish to retain control of the specific secrecy provisions relevant to departmental legislation[441].

7.6 The Committee's view on general provisions

7.6.1 The Committee considers that the arguments in support of the general provisions outweigh the factors in support of retaining the specific provisions. General provisions located in one statute provide a central focus. They are readily accessible and mean that officers only have to be familiar with one set of obligations. Thus, general provisions may assist in raising the consciousness of public servants as to their obligations in protecting the confidentiality of information acquired in the course of their duties. Such provisions are also readily accessible to the general public and clearly show that certain conduct (such as soliciting the disclosure of protected information from public servants) is unlawful.

7.7 Location of general provisions

7.7.1 The location of general provisions was commented upon in some submissions. The Privacy Commissioner suggested that a general offence of soliciting protected personal information held by Commonwealth agencies should be included in the Privacy Act.[442] The Victorian Council for Civil Liberties agreed that criminal offences and penalties relating to the protection of confidential personal data should be included in the Privacy Act.[443] However, it was noted that any suggestion to include criminal sanctions for unauthorised disclosure of confidential information by individuals in the Privacy Act was

---

439 ibid., p. S389. However, in those circumstances and according to the Prosecution Policy of the Commonwealth, it is unlikely that a person would be prosecuted unless the prosecution was in the public interest and there was a reasonable prospect of conviction.

440 ibid.

441 See Attorney-General's Department, *Transcript*, p. 175.

442 *Submissions*, p. S584.

443 *Submissions*, pp. S154–S155.

inconsistent with the structure of that Act.[444] The DPP suggested that if a single provision were enacted and supported by criminal sanctions, the logical placement of it would be in the Crimes Act.[445]

7.7.2 The Committee considers that the most appropriate location of any general offence provisions is the Crimes Act. Location in the Crimes Act 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 included in another statute. The stigma of a conviction under the Crimes Act would also appear greater than a conviction for violation of a secrecy provision under another Act.

7.7.3 The Committee therefore, does not agree with the Gibbs proposal that only the disclosure of 'official' information should be dealt with in the Crimes Act and the disclosure of other confidential information should not be the subject of a general criminal law. However, the Committee does agree that the protection of third party information should be dealt with separately from the protection of official information rather than the inclusion of both in a broad provision. The Committee concludes that the protection of confidential personal and commercial information should be the subject of a general criminal law.

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*.

7.8 Options for rationalisation

7.8.1 In the last twenty years there have been numerous inquiries which have considered Commonwealth secrecy provisions.[446] The Committee was informed that recommendations to expand the range of activities covered by specific provisions and to consolidate the prohibited conduct in one provision have been made on a number of previous occasions.[447] However, it was noted in the public hearings that while such

444 Department of Immigration and Ethnic Affairs, *Submissions*, p. S905.

445 *Submissions*, p. S1075.

446 The scope of these inquiries is outlined by the Attorney-General's Department in *Submissions*, pp. S370–S376.

447 Attorney-General's Department, *Transcript*, pp. 174–175.

proposals have been recommended previously, they have never been implemented.[448] It was suggested that reform:

> . . . would be more achievable under one provision, in that there would be a greater focus to the work in putting the recommendation forward and seeing it through the appropriate governmental processes.[449]

There is an obvious need for rationalisation and clearly this need has been recognised in the past.

7.8.2 The Committee has identified two options for the rationalisation of the existing secrecy provisions, namely consolidation and partial consolidation in the Crimes Act.

7.9 Option 1 – Consolidation

a) The approach

7.9.1 This option involves locating all of the offence provisions which protect 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. As discussed in chapter 4, exceptions to the prohibitions (that is, lawful transfers) should not be regulated by secrecy provisions.

7.9.2 From a theoretical perspective, consolidated provisions in one statute protecting all confidential commercial and personal information held by the Commonwealth Government and its agencies would be highly desirable. Such provisions would provide a central focus, consistency in approach and the obligations of individuals would be readily identifiable. The approach would also allow the repeal of the existing secrecy provisions in various statutes and this would simplify the relevant law. [450]

b) Assessment of option 1

7.9.3 While the Committee appreciates the benefits of consolidation, it also recognises that consolidation would be a difficult in practical terms. There may be doubt as to whether a description of 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

---

448 ibid.

449 ibid.

450 See Attorney-General's Department, *Submissions*, p. S389.

in departmental legislation rather than vest that function in the Crimes Act.[451] Thus there may be difficulties in obtaining broad inter-departmental agreement and approval for totally consolidated provisions in the Crimes Act.

7.9.4 While the Committee favours rationalisation of the current law, it is unsure whether consolidation is either practical or possible. In all the circumstances, the Committee therefore favours option 2.

7.10 Option 2 – Partial consolidation

a) The approach

7.10.1 The Attorney-General's Department suggested that an option may be to include a general provision in the Crimes Act which attaches criminal sanctions to conduct by reference to other enactments. For example, the Crimes Act provision could provide that acts prescribed by certain statutes listed in a schedule attract a penalty.[452] When a new provision is enacted, the schedule would be amended. It was suggested that this model:

> '. . . get[s] the best of both worlds in that you would direct attention to a central provision and at the same time maintain the flexibility that is needed for defining the conduct.'[453]

The Committee has termed this 'partial consolidation'.

7.10.2 While the Committee believes the approach suggested by the Attorney-General's Department has merit, it favours a variation of it. Unless the unlawful acts are proscribed in the Crimes Act, the approach will not overcome the current problem, namely that all specific statutes do not adequately protect third party information (for example, many statutes do not contain provisions which prohibit soliciting or offering to supply third party information).

7.10.3 The Committee favours an approach where the Crimes Act contains provisions prohibiting the relevant conduct. This would avoid the problem where officers who disclose information under one enactment, or a person who solicits information from one particular agency, may face prosecution while those who disclose the same information

---

451 This concern was averted to in DSS, *Submissions*, p. S449 and the Law Society of New South Wales, *Submissions*, p. S859.

452 *Transcript*, pp. 509–510.

453 *ibid.*

under a different enactment, or who solicit equally sensitive information from another agency, are not liable to prosecution.

7.10.4 Under this proposal, the offences relevant to each type of conduct would have common elements. This contrasts with the current situation where the offences have different elements depending on the specific statute which applies and some statutes do not legislate for the whole range of possible conduct.

7.10.5 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 as that description would be retained in departmental legislation. Given that the protected information is obtained under coercion pursuant to departmental legislation, it is logical for the departments to retain responsibility for the description of that protected information.

7.10.6 The penalties for the general offences would also be located in the Crimes Act. There would be one maximum penalty for each offence rather than the varying penalties which currently exist in the specific provisions. This would assist in promoting consistency in penalties.

7.10.7 The Committee notes that the maximum penalty for the relevant offences under the Social Security Act is two years imprisonment (or a $12 000 fine or both[454]). This is also the maximum penalty for offences under section 70 of the Crimes Act and most of the other relevant provisions in that Act. The Committee considers that a maximum penalty of 2 years imprisonment may be appropriate for the general offences it has recommended for inclusion in the Crimes Act.

7.10.8 Subsection 38(1) of the *Freedom of Information Act 1982* is an example of a provision which refers to other enactments.[455] Section 38 details one category of documents which are exempt from disclosure under the Freedom of Information Act. Subsection 38(1) provides the circumstances in which certain secrecy provisions apply to prevent disclosure of a document, or information contained in a document. The secrecy provisions to which this provision refers are listed in Schedule 3 of the Act. The document is an exempt document if disclosure is prohibited by a secrecy provision in

454 By virtue of subsection 4B(2) of the Crimes Act.

455 *Transcript*, pp. 509–510.

Schedule 3 or if it is expressly provided that subsection 38(1) of the FOI Act applies to the document or relevant information.

7.10.9 Section 75 of the *Insurance Acquisitions and Takeovers Act 1991* provides a variation of this approach and is an example of a provision which creates an offence by referring to an offence provision in a more general enactment. Subsection 75(1) of the Act provides that the object of the section is to create duties of non-disclosure for the purposes of section 70 of the Crimes Act. Subsection 75(2) details the prohibition on disclosure and subsections 75(3) and 75(4) provide exceptions to that prohibition. Thus a duty of non-disclosure is created by the departmental legislation and the relevant offence and penalty are those in section 70 of the Crimes Act. Partial consolidation would involve referring to the Crimes Act for the relevant offences and penalties in a similar manner to that in the Insurance Acquisitions and Takeovers Act.

b) Assessment of option 2

7.10.10 This option has the benefits of option 1, including consistency, clear identification of the obligations on individuals and promotion of a uniform standard for all Commonwealth officers. The advantage of option 2 is that it is a flexible way of centralising the existing secrecy provisions in the Crimes Act without reducing the control of the various departments over the information they protect. By referring to information defined in other enactments, there would be no need for an all-inclusive formula defining the information which should be protected.

7.10.11 The Committee recognises that implementation of this option will be a major undertaking as new offence provisions in the Crimes Act will need to be drafted and consequential amendments to a large number of secrecy provisions in the various statutes will also be required. The Committee also recognises that some departments have regimes dedicated to ensuring third party information is protected (for example, DSS and the ATO). However, in all the circumstances, 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 and its agencies 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.

7.11 Conduct that should be prohibited

7.11.1 The issue which now arises is the conduct that should be prohibited by the general offence provisions in the Crimes Act. The ICAC Report commented that confidential information should be protected at every point on the distribution chain.[456] The Privacy Commissioner agreed that each of the steps in the chain of activity should be prohibited. He noted that the Social Security Act has attached offences to many of these steps.[457] The various points on the distribution chain include accessing, disclosing, obtaining, procuring, soliciting, offering to supply and publishing confidential information. The ICAC Report adopted a global term 'unauthorised dealing' to describe the prohibited conduct.[458]

7.11.2 It is noted that, if committed, the offences associated with the original access to, or disclosure of, confidential third party information would be committed by public servants. The offences which are committed further along the distribution chain may be committed by either public servants or other individuals.

7.11.3 The ICAC Report suggested that the provisions of the Social Security Act could provide a basis for legislation to apply generally to protected government information.[459] The Social Security Act has been amended since publication of the ICAC Report. It currently contains the following offences: gaining unauthorised access to protected information[460], unauthorised use of protected information (including disclosing, recording or otherwise using)[461], soliciting the disclosure of protected information[462], soliciting disclosure by making untrue representations[463], offering to supply protected information[464] and holding oneself out as being able to supply protected information[465].

---

456 *ICAC Report*, op. cit., p. 219. See also Mr Roden, *Submissions*, p. S39.

457 *Transcript*, p. 479.

458 *ICAC Report*, op. cit., pp. 171, 218.

459 op. cit., p. 175.

460 Section 1312A of the Social Security Act.

461 Section 1312B of the Social Security Act.

462 Section 1316 of the Social Security Act.

463 Section 1316A of the Social Security Act.

464 Subsection 1318(1) of the Social Security Act.

465 Subsection 1318(2) of the Social Security Act.

7.11.4 The prohibition against unauthorised use of protected information in the Social Security Act was recently extended to information obtained by innocent means.[466] The Explanatory Memorandum cites two examples where information may be obtained by innocent means: if Departmental papers are found in a street or at the tip (because of a fire or defective disposal arrangements) or if information is incorrectly released by the Department (for example, an incorrectly addressed fax message).[467] However, no offence is committed unless the person finding the information knows (or ought reasonably to know) that it is protected and proceeds to intentionally record, disclose or otherwise use it. Possession or receipt does not itself constitute an offence unless the other elements of the offence are satisfied.

7.11.5 The AFP appears to consider that the onus of proof should be reversed and the law should require that any person who is in possession of confidential information, or who publishes it, to satisfactorily account for its possession.[468] Mr Roden suggested that if the nature of the information is established and the person is aware of its nature, then the dealing in that information should be an offence without it being necessary to establish the circumstances in which it came onto the market.[469] He also suggested that a reverse onus of proof should be considered in relation to the possession of protected information.[470]

7.11.6 The Attorney's General Department commented what while it was not a general policy to reverse the onus of proof, it is recognised that there are circumstances where it is appropriate.[471] A reversal of the onus of proof may be appropriate where the matter to be proved is peculiarly within the knowledge of the defendant. The Department appeared to view the possession of confidential information as a borderline case[472] and noted that reversing the onus of proof in this situation would go a long way to solving the problems that may arise in prosecutions when the alleged offender says 'I had no idea where the information came from' or 'I didn't ask where the information came from'.[473]

---

466 Section 1312B amended by section 15 of the *Social Security Legislation Amendment Act 1994* (No. 63, 1994).

467 Explanatory Memorandum, p. 19.

468 *Submissions*, p. S990 and *Transcript*, pp. 331–332.

469 *Transcript*, pp. 5–6.

470 *Transcript*, p. 6. See also *ICAC Report*, op. cit., p. 171.

471 *Transcript*, p. 176.

472 ibid.

473 See discussion between Committee Members and Attorney-General's Department officers at *Transcript*, p. 176.

7.11.7 The Committee has long been an advocate of protecting the rights of the accused. It believes that a decision to reverse the onus of proof should only be made in exceptional circumstances. However, the Committee also recognises the need to protect third party interests. In balancing these concerns, the Committee considers that an innocent recipient of confidential information should not be liable to prosecution by reason only of possession of the information. However, criminal liability should attach if that person has the requisite mental element and proceeds to use, disclose or make a record of the confidential information.[474] This applies equally to second, third and later recipients in the distribution chain.[475]

7.11.8 The publication of confidential third party information was the subject of some comment. The Privacy Commissioner suggested that any law should include prohibitions on publishing and disseminating confidential third party information.[476] The Attorney-General's Department noted that most Commonwealth legislation:

> . . . does not pick up subsequent use of the material after it has... left the hands of the Commonwealth employee. For example, . . . [there is] nothing that would allow us to prosecute a newspaper.[477]

7.11.9 In its submission, the Australian Press Council proposed that the media be given an immunity from civil or criminal liability for offences concerning misuse of confidential information in the following circumstances:

- where there is an unlawful disclosure of confidential personal or commercial information to the media;
- that information is published;
- the publication is in the public interest, being a matter of serious concern or benefit to the public; and
- the media is not itself guilty of criminal or tortious conduct.[478]

It appears curious that it is a defence to criminal or civil liability if certain conditions are satisfied when one of those conditions is that the media has not been involved in the criminal or tortious conduct. Presumably the defence would not need to operate unless the media concerned had committed a crime or was involved in tortious conduct.

---

474 See section 1312B of the Social Security Act.

475 See comment on lack of provisions covering third and fourth parties in distribution chain at *Transcript*, p. 174.

476 *Transcript*, p. 478.

477 *Transcript*, p. 174.

478 *Submissions*, p. S596.

7.11.10 The Committee finds it difficult to see why confidential third party information published by the media should not be subject to criminal sanctions when the persons previously involved in the distribution chain would be subject to such sanctions.[479] The Committee considers that there is no justification for a public interest defence in these circumstances.

7.11.11 It was submitted that another area in which the existing criminal law may be deficient is with respect to the improper use of information.[480] The report of the Committee of the Inquiry on Public Duty and Private Interest (the Bowen Committee) noted that section 70 did not extend to situations where an officer, or a former officer, misuses government information himself or for his own advantage without actually disclosing it.[481] The Committee recommended that a proscription on the misuse of government information should be included in the Crimes Act.[482]

7.11.12 In this connection, the Gibbs Committee recommended the creation of a new offence of using, in a dishonest way, any information acquired by a Commonwealth officer by virtue of his or her position followed by a series of non-exhaustive illustrations. One illustration of the offence that the Gibbs Committee gave related to the use of information, which is generally not freely available, concerning the value of a property and the use of that information caused the property to be acquired or disposed of.[483] In making this recommendation, the Gibbs Committee stated that the offence should not be confined to the specific categories of official information previously defined.[484] Thus this recommendation goes beyond the realm of purely 'official' information and is relevant to third party information. The Committee supports this recommendation of the Gibbs Committee and understands that the Government is currently considering this proposal.

---

479 The Committee notes the Government's recent announcement, in its response to the Commission of Inquiry into the Australian Secret Intelligence Service, that liability in relation to the disclosure of *official* information will extend to secondary disclosures. See Statement of Senator the Hon Gareth Evans, Minister for Foreign Affairs, Senate, *Hansard*, 1 June 1995, p. 722 (proof issue).

480 Attorney-General's Department, *Submissions*, p. S389.

481 *Report of the Committee of Inquiry into Public Duty and Private Interest* PP 353/1979, para 14.19.

482 ibid., para 14.20. This recommendation was criticised by Professor Finn in *Official Information*, op. cit., p. 209.

483 *Final Report*, op. cit., p. 361 cited in Attorney-General's Department, *Submissions*, p. S389.

484 *Final Report*, op. cit., p. 361.

7.11.13 The Gibbs Committee also considered that there should be an offence of dealing with the disclosure of protected information by non-public servants. However, that offence was to apply only to the specific categories of information which would be protected under the Committee's proposed provisions[485] (that is, relating to the protection of official information). Implementation of the Committee's next recommendation in relation to prohibiting unauthorised dealing at every stage of the distribution chain would ensure that unauthorised dealing in confidential third party information by non-public servants is prohibited.

7.11.14 The ICAC report recommended that, 'unauthorised dealing in protected government information be made a criminal offence' in New South Wales.[486] 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. 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.

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*.

7.11.15 In discussing the law relating to the protection of confidential information, the ICAC Report commented that it is imperative that every effort be made to achieve consistency between the States and the Commonwealth.[487] The Committee suggests that consideration should be given to promoting consistency in the laws concerning the protection of third party information held by the Commonwealth Government and its agencies, and the laws concerning similar information held by State Governments and their agencies.

485 Attorney-General's Department, *Submissions*, p. S392.

486 *ICAC Report*, op. cit., pp. 171, 218.

487 ibid., p. 172.

Chapter 8

Remedies and the need for compensation

The Privacy Act overcame certain defects in the general law of confidence in relation to personal information. The Privacy Commissioner closed some 250 privacy complaints in 1993–94. The effectiveness of the negotiation process of settlement is such that in only two cases did he find it necessary to issue a determination.

It is not constitutionally possible for the Privacy Commissioner to be vested with power to award damages against individuals who procure unauthorised disclosures of personal information. The Committee proposes that it should be possible however, for an individual to establish a right to compensation from a Commonwealth agency by the fact of the unauthorised disclosure even where the agency has not been in breach of the IPPs.

8.1 Introduction

8.1.1 A legal remedy is the means by which the violation of a right is prevented, redressed or compensated and its purpose is to benefit the person whose right is threatened, rather than to punish the person who has committed a wrong. Remedies might include breach of contract, breach of fiduciary obligations, negligence, trespass, conversion, nuisance and deceit. Although there is no general right to privacy, remedies are available to third parties in circumstances where information relating to them has been wrongly disclosed under both the existing common law and statute law.[488] More specifically, the Attorney-General's Department identified that remedies were available under the *Privacy Act 1988* and the general law of confidence.[489]

8.2 General law of confidence

8.2.1 Although the common law does not recognise a tort of violation of privacy. As mentioned in chapter 2, the common law and equity provide remedies for the improper use of confidential information. There are three main ways in which a duty to maintain

488 Although they are not discussed here, the Committee recognises the significance of the provisions contained in the FOI Act that enable an individual who feels that a certain proposed disclosure of information would be wrong, an opportunity to prevent that disclosure from occurring. The IPPs reflect this approach to informing an individual about the use to which information about her or him is put. While it is clear that this step provides an individual with a remedy because it enables her or him to prevent a wrongful disclosure, this chapter focuses on the circumstances specified in the sixth term of reference – where information relating to an individual has already been wrongly disclosed.

489 Attorney-General's Department, *Submissions*, pp. S357 and S359 respectively.

the confidentiality of third party information may arise. First, the actual relationship between parties may give rise to a duty of secrecy, such as that between solicitor and client, or doctor and patient. Second, parties to a contract may agree that certain information is to be kept confidential. Finally, there are certain cases in which, by virtue of the nature of the information and the circumstances of its disclosure, an equitable obligation of confidence is imposed on the recipient of the information.

8.2.2 An obligation of confidence does not apply where the use or disclosure of the information is 'authorised or required by law'. The Attorney-General's Department stated that the Commonwealth has frequently legislated to extend the uses that can be made of third party information supplied to the government and, concluded that the circumstances where obligations of confidence apply in the Commonwealth sphere were limited.[490]

8.2.3 The Attorney-General's Department considered there to be a wide range of remedies available in a breach of confidence action.[491] They include injunctions, damages for breach of contract, compensation for breach of an equitable duty of confidence, and an account of profits. The Committee also received evidence about one case where the Ombudsman found a breach of confidence had occurred. Although no financial remedy was recommended, the Ombudsman found that a Commonwealth agency should apologise because it released confidential personal and commercial information.[492]

8.3 Some general law defects were overcome by the Privacy Act

8.3.1 In its 1983 report on Privacy, the Australian Law Reform Commission (ALRC) examined in detail the existing law of confidence with respect to the improper disclosure of public sector information. It found that:

> There appears to be little need for a legislative restatement of the circumstances in which a duty of confidence will arise, at least in relation to personal information. The law is clear. It confers a cause of action in circumstances that balances appropriately the relevant interests. It is still developing, and its growth should be guided, not stultified.[493]

8.3.2 The ALRC identified three defects in the general law on breach of confidence:

---

490 Attorney-General's Department, *Submissions*, p. S359.

491 Attorney-General's Department, *Submissions*, p. S359.

492 C. Mann, *Submissions*, p. S735.

493 Law Reform Commission, *Privacy (Vol 2)*, p. 146.

- where a person is under a duty to preserve confidentiality in respect of information about another person, the right to enforce that duty should be extended to that other person;
- it should be made clear that, as a general rule, personal information to which a duty of confidence applies should remain protected by that duty no matter into whose hands the information might subsequently fall;
- the basis of awarding damages should be clarified so that, both injunctions and damages, will be available to a person seeking to enforce the duty.[494]

8.3.3 These defects were remedied in relation to personal information held by the Commonwealth by virtue of the enactment of Part VIII of the Privacy Act. Section 93 of that Act provides that the subject of personal information which is disclosed has the same rights in relation to that improper disclosure as does the person who provided the information. It also clarifies that damages may be recovered for a breach of confidence. Section 92 provides that obligations of confidence pass on to any person who subsequently acquires the information.

8.3.4 The Committee considers that the law on breach of confidence is of importance in conferring remedies for third parties whose confidential information is wrongly disclosed.[495] In particular, Part VIII of the Privacy Act clarifies and strengthens the law on breach of confidence in relation to personal information held by the Commonwealth. The Committee also accepts the evidence from the Attorney-General's Department that the law on breach of confidence has limited practical application in the Commonwealth sphere and that rights arising from breaches of confidence may be difficult to enforce.

8.4 No common law or statutory tort of breach of privacy

8.4.1 In response to a question by the Committee the Attorney-General's Department expressed the opinion that 'there is no convincing indication that the courts in Australia are moving towards the development of a common law tort of breach of privacy'.[496]

8.4.2 Although the ALRC considered the option of creating a statutory general tort of invasion of privacy in its inquiry into privacy protection, that option was not

---

494 ibid., pp. 146–147.

495 For a recent example see *Johns v Australian Securities Commission (1993) 116 ALR 567.* In that case the High Court decided that the Australian Securities Commission had breached a duty of confidence when it disclosed to a Victorian Royal Commission transcripts of compulsory examinations of a director of the Tricontinental group.

496 Attorney-General's Department, *Submissions*, p. S1026.

recommended. The ALRC considered that '[s]uch a tort would be too vague and nebulous.' The ALRC further considered that general tort remedies are not always available to those in most need, '[t]hey are not a substitute for comprehensive measures for the protection of privacy such as are recommended in this report.'[497]

8.4.3 The Attorney-General's Department also commented that the enforcement of third party rights (arising from breaches of confidence) through the judicial system may be both protracted and expensive.[498]

8.4.4 At the time the Privacy Bill was debated the Honourable Lionel Bowen MP, the then Attorney-General, said that the government wanted to create a right of action that would be accessible to ordinary persons but would not unduly encourage litigation.[499]

8.4.5 The Annual Reports of the Privacy Commissioner indicate that the right of action under the Privacy Act is accessible to many persons.

8.5 The Privacy Commissioner's jurisdiction

8.5.1 An individual may complain to the Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual.[500] The Privacy Commissioner is to investigate an act or practice of an agency that may breach an Information Privacy Principle and to effect a settlement of the matters that gave rise to the investigation.[501]

8.5.2 The Privacy Commissioner may make a determination to dismiss a complaint, or if the Privacy Commissioner finds the complaint to be substantiated, a determination may be made to provide a remedy to the individual who complained.[502] Where a declaration involves monetary compensation for loss or damages, the matter is reviewable by the Administrative Appeals Tribunal.[503] Determinations against agencies are enforceable upon application by the Privacy Commissioner to the Federal Court of Australia.[504]

---

497 The Law Reform Commission, *Privacy*, ALRC 22, AGPS Canberra 1983, para. 1081.

498 Attorney-General's Department, *Submissions*, p. S399.

499 House of Representatives, *Hansard*, 3 November 1988, p. 2390.

500 Section 36 of the Privacy Act.

501 Section 27 of the Privacy Act.

502 Section 52 of the Privacy Act.

503 Section 58 of the Privacy Act.

504 Section 59 of the Privacy Act.

8.5.3 Since the commencement of the Privacy Act the Office of the Privacy Commissioner has received thousands of complaints. During 1993–94 there were 143 complaints lodged, 81 of which concerned breaches of the Information Privacy Principles. The Privacy Commissioner points out that the number of complaints recorded is a significant reduction on the number received in the previous reporting year.[505] This reduction was due in part to a greater use of the discretion not to continue to investigate a complaint on the ground that it had not first been made to the respondent.

8.5.4 During 1993–94, 250 privacy complaints were finalised and closed on a range of grounds. The grounds included:

- the respondent had adequately dealt with the complaint;
- there was no evidence of interference with the privacy of the complainant;
- the complaint was withdrawn or contact was lost with the complainant;
- the complaint was vexatious or frivolous;
- the complaint was referred elsewhere; and
- the Privacy Commissioner made a complaint determination.[506]

8.5.5 In those cases closed on the basis of the respondent adequately dealing with the complaint, a settlement was negotiated by the Privacy Commissioner's staff with the respondent, taking into account the complainant's views. The remedial action included apologies to the complainants together with revised procedures (including staff training) to minimise the risk of a future breach of the Privacy Act. In a number of cases specific action was taken in relation to the complainant, such as amending personal records and providing additional security in relation to those records. In a few cases individuals received monetary compensation, for non-economic loss associated with hurt and embarrassment or for lost wages following lost employment opportunities.[507]

8.5.6 In only two of the cases closed in 1993–94 did the Privacy Commissioner find it necessary to issue a determination. This reflects favourably on the overall effectiveness of the negotiation process of settlement.

8.5.7 Some witnesses were of the opinion that existing remedies were adequate.[508] No evidence was presented to the Committee that the compensation available under the

---

505 Privacy Commissioner, *Sixth Annual Report on the Operation of the Privacy Act – for the period 1 July 1993 to 30 June 1994*, AGPS Canberra 1994, p. 55.

506 Privacy Commissioner, *Sixth Annual Report on the Operation of the Privacy Act – for the period 1 July 1993 to 30 June 1994*, AGPS Canberra 1994, p. 57.

507 Privacy Commissioner, *Sixth Annual Report on the Operation of the Privacy Act – for the period 1 July 1993 to 30 June 1994*, AGPS Canberra 1994, p. 57.

508 Mr Gerald Ryan, *Transcript*, p. 65.

Privacy Act was inadequate. There was evidence however that the limitation on the Privacy Commissioner to provide a remedy only in those instances where an agency is found to have breached the IPPs reduced the effectiveness of existing remedies.

8.6 No remedy for certain disclosures

8.6.1 Despite the extension of remedies under the Privacy Act deficiencies remain. It is important to note that the remedies under the Privacy Act are only available where an agency is itself in breach of an IPP. For example, under IPP 4 an agency is required to adopt reasonable security measures to guard against unauthorised loss or disclosure of personal information. A breach of IPP 4 occurs if the Privacy Commissioner finds that an agency did not have reasonable security measures when a disclosure occurred.[509] The Privacy Commissioner stated that an unauthorised disclosure does not necessarily involve a breach of the IPP. Furthermore, he considered that in cases where large numbers of staff have legitimate access to personal data, it is not reasonable to expect a security system to entirely avert the possibility of unauthorised disclosure.[510]

8.6.2 Consequently, 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 the IPPs. A further deficiency exists, because under the Privacy Act the individual does not have any means of obtaining redress from parties to the disclosure other than the Commonwealth agency involved.

8.7 No liability in damages of those that procure improper disclosure

8.7.1 In the Privacy Commissioner's first and second annual reports, a recommendation was made that the Government consider amending the Privacy Act to impose liability in damages on those that procure the improper disclosure of personal information.[511]

8.7.2 The Senate Standing Committee on Legal and Constitutional Affairs considered this matter and recommended that the Government indicate, as a matter of urgency,

---

509 Mr K. O'Connor, *Transcript*, p. 491.

510 Privacy Commissioner, *Submissions*, p. S585.

511 *First Annual Report on the Operation of the Privacy Act-For the period 1 January 1989 to 30 June 1989*, p. 29; *Second Annual Report on the Operation of the Privacy Act-For the period 1 July 1989 to 30 June 1990*, p. 15.

what action it was taking, or proposed to take on the matter.[512] In its response, the Government stated that it did not support the extension of the Commissioner's powers to enable the award of damages against individuals involved in unauthorised disclosures. The proposal was at odds with the essential role of the Privacy Commissioner, that is, to oversee the collection, handling, use and disclosure of personal information by Commonwealth agencies. There were also constitutional limitations on the Commonwealth's ability to vest what may amount to judicial power in the office of the Privacy Commissioner.[513]

8.7.3 Advice from the Attorney-General's Department supports this opinion. The Department considers that, if the Privacy Act were amended to allow the Privacy Commissioner to award damages against individuals who procure unauthorised disclosures of personal information and the Privacy Act were amended to provide for awards to be enforceable without full review by a court, the amendment would be invalid on the ground that it purported to vest the Commissioner with judicial power contrary to Chapter III of the Constitution.[514]

8.7.4 The Department considered however, that the provisions under Division 3 of Part V of the Privacy Act could probably be applied. These provisions provide that a determination of the Privacy Commissioner against a non-Commonwealth agency may be registered with the Federal Court and may be enforced, but only after an opportunity by the defendant to have the matter fully investigated by the Federal Court. The Department indicated that similar provisions under the Racial Discrimination Act were subject to a High Court challenge on the ground that they purport to vest judicial power in the Human Rights and Equal Opportunity Commission contrary to Chapter III of the Constitution (*Harry Brandy v Human Rights and Equal Opportunity Commission*).[515] The High Court in that case subsequently held that the provisions in the Racial Discrimination Act were unconstitutional.[516] It would appear that the provisions of Division 3 of Part V of the Privacy Act would be invalid on the same ground.

8.7.5 In light of the *Brandy* Case, the Privacy Commissioner could not validly register with the Federal Court any determination to award damages against individuals and non-Commonwealth agencies who procure the improper disclosure of personal information.

---

512 *Unauthorised Procurement and Disclosure of Information*, p. 10.

513 *Senate Hansard*, 10 October 1991, p. 1821.

514 Attorney-General's Department, *Submissions*, p. S1018.

515 ibid., pp. 1018–1019.

516 *Harry Brandy* v *Human Rights and Equal Opportunity Commission*, High Court of Australia, 23 February 1995.

The Privacy Commissioner would also not be able to enforce such a determination. Because of this, the Committee considers that little would be achieved by proposing to extend the powers of the Privacy Commissioner to award damages against individuals and non-Commonwealth agencies who procure the unauthorised disclosure of personal information.

8.8 Strict liability in damages of agencies involved in improper disclosure

8.8.1 The Attorney-General's Department suggested that it would be appropriate for third parties to have more comprehensive access to compensation from Commonwealth agencies where information relating to them has been wrongly disclosed. The Department reasoned that greater recognition be given to the Commonwealth's responsibility to hold confidential material 'in trust' for the owners of that information.[517] As a consequence of this responsibility, where information is unlawfully disclosed, an individual should be entitled to some form of compensation from the agency holding that information based on the fact of unauthorised disclosure.

8.8.2 To this end, the Department suggested that a 'strict liability' regime be introduced, that is, a right to compensation from the agency which held the information would be established by the fact of unauthorised disclosure of the confidential information. Subject to any constitutional limitations, the scheme could be administered by the Privacy Commissioner or the Ombudsman.[518]

8.8.3 The Privacy Commissioner supported this suggestion as it would enable compensation to be paid to a complainant without having to establish that the agency had breached one of the IPPs.[519]

8.8.4 Dr June Factor, Committee Member of the Victorian Council for Civil Liberties, also agreed that affected persons in such cases need compensation:

> You can penalise the person who has used the information but still, at the end of the day, you have somebody traumatised by that experience and they ought to have some means of redress.[520]

---

517 Attorney-General's Department, *Submissions*, pp. S400–S401.

518 Attorney-General's Department, *Submissions*, p. S401.

519 Mr K. O'Connor, *Transcript*, p. 491.

520 *Transcript*, p. 149.

8.8.5 The decision in the *Brandy* case is not an obstacle to introducing such a scheme. Under the existing provisions of the Privacy Act, there is no requirement to register a determination against a Commonwealth agency with the Federal Court. It is assumed that in such cases the Commonwealth agency will comply with the determination.

8.8.6 The Committee considers that it is desirable for third parties to have more comprehensive access to compensation from Commonwealth agencies where confidential personal information they hold is wrongly disclosed. This is so in light of the unlawful activities of Commonwealth officers revealed by ICAC. 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.

Chapter 9

Appropriateness of provisions governing access to third party information

This chapter discusses access to third party information through the Archives Act and the Freedom of Information Act. Under the provisions of the Archives Act, access to information relating to personal affairs is not permitted in the 'open access period' if the disclosure would be unreasonable. Open access to records is permitted after the records have been held for 30 years.

This chapter also considers access to public register information, particularly access to information contained on the electoral roll. The concern with access to public information is that information technology allows the information to be used for purposes in addition to that for which it was collected. The chapter concludes by discussing access to medical records for statistical and research purposes. The discussion focuses particularly on the collection of data by state cancer registries, its release to the Australian Institute of Health and Welfare and potential access to this information by external researchers.

9.1 Introduction

9.1.1 Paragraph (g) of the terms of reference requires the Committee to examine:

> 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 relevant 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 details the length of time information acquired by the Government must be treated as confidential and outlines the circumstances under which documents may be exempted from release. The FOI Act establishes a right of access to Government information. Access to third party information held by the Government may also be affected, in limited circumstances, by the general law on breach of confidence.[521] The administrative mechanisms which deal with access to, and the protection of, third party information are referred to in chapter 3 (and include physical security, staff training and the nurturing of a privacy culture) and chapter 7[522].

521 See chapter 8.

522 See paragraph 7.2.4.

9.1.2 In this chapter, the Committee will outline and discuss the schemes under the Archives Act and the FOI Act. It will also examine access to particular types of information, including public registers and access to information contained in medical records for statistical and research purposes.

9.2 Archives

9.2.1 Australian Archives is responsible for the broad management of the records of a majority of the agencies of the Commonwealth Government, particularly in relation to the control, accessibility, disposal and storage of those records.[523] The functions of Australian Archives include ensuring the preservation of existing archival resources and encouraging the use of archival material.[524]

9.2.2 Archives are preserved explicitly for use by third parties for purposes other than those for which the records were created. The existence of archives, therefore, represents a prima facie breach of privacy and confidentiality principles allowing the use of information by third parties for purposes other than those for which the record of that information was created.[525]

9.2.3 The Australian Society of Archivists noted that in relation to archival material, there must be a balance between the protection of personal and commercial information and the public interest in allowing legitimate research.[526] The Society suggested that the community's interest in supporting third party research subject to access polices – expressed though the establishment of archival institutions - represents a legitimate countervailing public interest to privacy principles which limit the use of personal information to the purpose for which it was created.[527]

9.2.4 Prior to 1970 Commonwealth records were generally withheld from public access for 50 years. The introduction of the 30 year general rule resulted in the establishment of comprehensive procedures for identifying sensitive information.[528] Australian Archives has generally undertaken the task of examining records to see whether certain

---

523 Australian Archives, *Submissions*, p. S303. Australian Archives is established under Part II of the Archives Act.

524 See subsection 5(2) of the Archives Act.

525 See Australian Society of Archivists Incorporated, *Submissions*, p. S107.

526 ibid., p. S107.

527 ibid., p. S109.

528 See Australian Archives, *Submissions*, p. S304.

categories of information should be withheld beyond 30 years. However, some departments and agencies determine whether their own records (relating to defence, security, international relations and Cabinet material) should be withheld.

9.2.5 The Australian Archives have developed guidelines for the identification of sensitive material, including that related to personal privacy. These guidelines are included in the Australian Archives Access Manual.[529]

a) The *Archives Act 1983*

9.2.6 The Act created a statutory right of public access to Commonwealth records that were more than 30 years old (with some exceptions). As outlined in chapter 2, the Act established procedures to provide public access to Commonwealth records in the 'open access period', that is, after the 30 year time period (from 31 December in the year in which the record came into existence) has elapsed.[530] The Privacy Act and the Information Privacy Principles contained in that Act do not apply to records in the open access period. The exclusion of such principles recognises that over time certain classes of personal information may no longer retain their original sensitivity.[531]

9.2.7 Section 33 of the Act details the categories of material which are 'exempt records' and are therefore not publicly available after the thirty year period has elapsed. Notwithstanding the exemptions, section 38 of the Act provides that, where reasonably practicable, Australian Archives may make arrangements for partial access to an exempt record where access can be given without disclosing the information or matter which made the record exempt. If an application for access, or an extension of partial access, to records in the open access period is refused, mechanisms exist to review the decision.[532] The exemption and appeal provisions are based on those in the FOI Act.

9.2.8 The Archives Act has recently been amended to prevent the inadvertent removal of records from the operation of the Archives Act as a consequence of a change in the structure of certain enterprises.[533] The amendments provide that bodies which are established for a public purpose or subject to Commonwealth control remain subject to the Archives Act unless specifically excluded from the operation of the Act. The

---

529 ibid., p. S304. Relevant extracts from that Manual are set out at *Submissions*, pp. S308–S328.

530 See subsection 3(7) of the Archives Act.

531 Australian Archives, *Submissions*, p. S305.

532 See Division 4 of the Archives Act.

533 Mr Lindsay, Second Reading Speech on the Archives Amendment Bill 1995, House of Representatives, *Hansard*, 1 March 1995, p. 1360.

amendments also provide that prior records of bodies which are removed from the application of the Act remain subject to the Act unless specifically excluded from its application.[534] It was noted that the amendments are not intended to ensure that all Commonwealth records remain subject to the Archives Act, but rather to ensure that the disposition of such records is addressed as part of the sale process.[535]

b) The protection of personal information

9.2.9 The majority of Commonwealth records are destroyed when they are no longer needed. Decisions on whether the records should be retained are based on their informational value and not their sensitivity.[536] There are three types of records which contain personal information and which may be retained by Archives. Those records are:

- records which deal essentially with policy or administrative matters but which include some personal information;
- records which document an individual citizen's dealings with government on matters which have some degree of sensitivity (for example, migrant naturalisation files and employment or education records); and
- individual case files of high sensitivity (that is, medical or welfare files including, for example, repatriation case files) which may form an important social or medical record of Australian social history.[537]

9.2.10 The exempt records detailed in section 33 of the Act, which are not released after the thirty year period, include a number of categories of information relevant to the protection of third party information. Those categories include:

- information or matter where disclosure would constitute a breach of confidence;[538]
- information or matter where disclosure would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person);[539]

---

534 ibid., pp. 1360–1361. The *Archives Amendment Act 1995* inserted the amendments in the Archives Act. The relevant provisions were assented to on 15 March 1995 and were proclaimed on 7 June 1995 (*Special Gazette No. 201*).

535 Mr C. Hollis, House of Representatives *Hansard*, 1 March 1995, p. 1363.

536 Australian Archives, *Submissions*, p. S303.

537 ibid., p. S304.

538 Paragraph 33(1)(d) of the Archives Act.

539 Paragraph 33(1)(g) of the Archives Act.

- information or matter which relates to trade secrets or any other information with a commercial value which may be destroyed or diminished if the information is disclosed;[540]
- information or matter concerning a person in respect of his or her business or professional affairs or information concerning the business, commercial or financial affairs of an organisation or undertaking, where disclosure would, or could reasonably be expected to, unreasonably affect the person adversely in respect of his or her business or professional affairs or an organisation or undertaking in respect of its lawful business, commercial or financial affairs[541]; and
- information or matter which relates to the personal, business or professional affairs of any person or that relates to the business, commercial or financial affairs of an organisation or undertaking and a taxation law prohibits disclosure of information or matter of the kind described[542].

9.2.11 In relation to personal affairs, the sole criterion for deciding whether access should be given to such information under paragraph 33(1)(g) of the Act is whether the disclosure would constitute an unreasonable disclosure of an individual's affairs.[543] The *Australian Archives Access Manual Part 1* considers the meaning of 'unreasonable disclosure in relation to personal affairs' in the context of the Act. The Manual notes that the issue is a matter of individual perception and rarely subject to a consensus of views.[544]

9.2.12 The recognition of certain classes of information as subject, or not subject, to paragraph 33(1)(g) of the Act is often not difficult. For example, the disclosure of innocuous information (such as basic identity details) is not unreasonable and such information would not be an exempt record under section 33. However, it may be unreasonable to allow the disclosure of information which is highly sensitive (such as medical details), at least in the lifetime of the person concerned (and perhaps even in the lifetime of that person's children).[545]

9.2.13 The Manual notes that the category of information which is the most problematic from the point of view of public access is that which falls between those two extremes.

---

540 Paragraph 33(1)(h) of the Archives Act.

541 Paragraph 33(1)(j) of the Archives Act.

542 See subsection 33(3) of the Archives Act.

543 Australian Archives, *Submissions*, p. S322.

544 ibid.

545 ibid.

This information may include single items of biographical data or an aggregation of details about a person. There is no clear agreement on the sensitivity of this type of information.[546] Determining whether the disclosure of certain information relating to personal affairs is unreasonable is clearly a subjective assessment. Consequently, Archives seeks to apply consistent standards to the release or exemption of personal information. Where the subject's wishes are unknown, the disclosure or exemption of certain personal information '. . . is determined by reference to a set of common principles based on the perceived reaction of the "reasonable person" '.[547]

9.2.14 The Archives policy on the release of personal information is based on the principle that it is not unreasonable to release basic information about named individuals after 30 years. This information includes date and place of birth, educational qualifications, employment history, religion, details of immigration and naturalisation and readily observable physical characteristics such as height, weight, complexion, visible scars and deformities. Information concerning criminal convictions (where the case was heard in open court) is generally released, although aggregations are usually not released.[548]

9.2.15 As outlined in the *Australian Archives Access Manual*, the following information is assessed according to its context and content: political affiliations and beliefs, character assessments, ASIO and police dossiers and censored mail. The following information is generally not released:

- financial history, such as debts and credit ratings[549];
- medical information (at least during the known or assumed lifetime of the subject), although isolated references to minor ailments or injuries may be released earlier[550];
- personal relationships including marital problems, sexual preferences, domestic violence, incest, adoption, illegitimacy, prostitution[551];
- intellectual capacity (such as the results of IQ tests)[552];
- transcripts of telephone intercepts[553]; and

546 ibid.
547 ibid., p. S323.
548 ibid., pp. S306, S328 (extracts from the *Australian Archives Access Manual*).
549 ibid., p. S328.
550 ibid., pp. S305, S328.
551 ibid., pp. S306, S328.
552 ibid., p. S328.
553 ibid.

- information provided in confidence to government authorities (for example, information concerning tax evasion, welfare fraud and criminal matters)[554].

c) The adequacy of the Act

9.2.16 As at 1992, Archives had only received a small number of internal reconsideration applications relating to personal privacy exemptions and none of those applications proceeded to the AAT.[555] Archives also noted that it had not received any complaints from members of the public about personal information released under the Act.[556] From this, Archives concludes that the access policy currently being applied to personal information in Commonwealth archival records is in line with general community attitudes.[557]

9.2.17 The Privacy Commissioner commented that given the public access exemptions, the provision for release of formerly confidential information held by the Commonwealth does not raise major privacy concerns and no privacy breaches arising from the operation of the Archives Act had been reported to the Privacy Commissioner at that time.[558]

9.2.18 However, the Privacy Commissioner did comment on the use of the term 'personal affairs' in the Archives Act and stated that it is important the term is sufficiently broad to cover all personal information which could be regarded as privacy sensitive.[559] Prior to 1991 the term 'personal affairs' was used in the FOI Act. That term was given a relatively restricted interpretation by the AAT in several cases[560] and the FOI Act was subsequently amended to replace 'information relating to personal affairs' with 'personal information' which was viewed as a broader term.[561] The explanatory memorandum to the FOI amending legislation described 'information relating to personal affairs' as a limited and uncertain expression.[562]

---

554 ibid.

555 ibid., p. S306. Australian Archives informs that this is still the case. However, the personal privacy exemption has been a subsidiary issue in some cases.

556 Archives informs that this is still the case.

557 ibid., pp. S306–S307.

558 As at October 1992. See *Submissions*, p. S592.

559 ibid.

560 See, for example, *Re Williams and Registrar of the Federal Court of Australia* (1985) 8 ALD 219 and *Re Dyrenfurth and Department of Social Security* (1987) 12 ALD 577 [appeal allowed in *Department of Social Security* v. *Dyrenfurth* (1988) 80 ALR 533].

561 Privacy Commissioner, *Submissions*, p. S592.

562 Explanatory Memorandum to the Freedom of Information Amendment Bill 1991, pp. 2, 13 contained in House of Representatives, *Bills* 36th Parliament, Session 1990–91–92–93, vol. 12.

9.2.19 This amendment brought the terminology of the FOI Act in line with that in the Privacy Act in this respect. 'Personal information' is defined in the FOI Act and the Privacy Act as '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'.[563]

9.2.20 The Privacy Commissioner considered that it may be desirable to amend the Archives Act in a manner similar to the FOI Act.[564] The Committee considers that, in the interests of consistency, it may be desirable to replace references in the Archives Act to 'information relating to the personal affairs of any person' with 'personal information about any person' and insert the same definition of 'personal information' in the Archives Act as is found in the FOI and Privacy Acts.

> *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*.

9.3 *Freedom of Information Act 1982*

9.3.1 The FOI Act establishes a general right of access to government information. The object of the Act is to extend as far as possible the right of the Australian community to access to information in the Commonwealth Government's possession.[565] The right of access is, however, subject to certain exemptions. The Act provides that the right of access to information should be limited only by those exemptions necessary for the protection of the public interest and the private and business affairs of persons (in respect of whom information is collected and held by departments and public authorities).[566]

---

563 See subsection 6(1) of the Privacy Act and subsection 4(1) of the FOI Act.

564 Privacy Commissioner, *Submissions*, p. S592.

565 Subsection 3(1) of the FOI Act.

566 See paragraph 3(1)(b) of the FOI Act.

9.3.2 The exemptions are a qualification of the right to access provided under the Act. Those exemptions that are particularly relevant to the protection of third party information include documents affecting personal privacy[567], documents relating to business affairs[568], documents to which certain secrecy provisions apply[569] and documents which contain material obtained in confidence[570]. Subject to certain narrow qualifications, the exemptions in the FOI Act do not generally prevent disclosure to the individual or organisation which is the subject of the claim for exemption.

9.3.3 Access to documents under the FOI Act is generally not provided unless the third party has had an opportunity to make submissions in support of the contention that the document should be exempt from disclosure.[571] Where a decision is made to release the documents despite the submissions of a third party, the third party may appeal to the AAT in respect of the decision.[572]

9.3.4 The Committee notes that a review of the Freedom of Information Act is currently being conducted by the Australian Law Reform Commission and the Administrative Review Council. A discussion paper on this matter was released in May 1995. The Review discusses whether there are some exemptions that agencies should not be able to waive. It suggests that where an exemption protects the interests of individuals or businesses, it may not be appropriate for the exemption to be waivable.[573] The Review proposes that agencies should not be able to waive the exemptions in subsection 37(1)(c)[574] and sections 41[575] and 43[576] of the FOI Act, in relation to persons other than the government and GBEs because it is inappropriate for the government to waive protection afforded to third parties.[577] The Review also queries whether there are

---

567 Section 41 of the FOI Act.

568 Section 43 of the FOI Act.

569 Section 38 of the FOI Act.

570 See section 45 of the FOI Act. Note that the FOI 'breach of confidence' exemption is in line with the general law on breach of confidence.

571 See section 27 of the FOI Act for the procedure concerning documents relating to business affairs and section 27A for the procedure concerning documents containing personal information.

572 See section 59 of the FOI Act for review of decisions concerning documents relating to business affairs and section 59A for review of decisions concerning documents containing personal information.

573 ALRC and ARC, *Freedom of information*, Discussion Paper 59, May 1995, p. 49.

574 Subsection 37(1)(c) relates to a document which would, or could reasonably be expected to, endanger the life or physical safety of any person.

575 Section 41 relates to documents affecting personal privacy.

576 Section 43 relates to documents concerning business affairs etc.

577 ibid.

other exemptions that should be non-waivable.[578] The Committee supports the view that agencies should not be able to waive the exemptions outlined by the Review. Disclosure of some information may have such serious repercussions that claiming the exemption should not be discretionary. The final report on the Review of the FOI Act is scheduled to be provided to the Attorney-General in December 1995.

9.4 Period of confidentiality and the appropriateness of disclosure

9.4.1 During its examination of the Archives Bill 1978, the Senate Standing Committee on Legal and Constitutional Affairs accepted that personal privacy is an interest that may warrant protection for longer than thirty years.[579] The Act recognises that third party interests may still be affected after that time and caters for it in the categories of exempt records.

9.4.2 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.[580] As noted by the Department, this is recognised in existing schemes.[581] Examining the interest 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 exemption to public access to personal information is 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.[582]

9.4.3 The ATO outlined circumstances relevant to its operations where the disclosure of certain information would be inappropriate. The ATO noted that all information acquired by it is confidential. The confidentiality of information held by the ATO and a taxpayer's liability do not alter after a period of time has elapsed. In relation to taxation fraud, the ATO is not limited in time in relation to the raising of assessments to collect

---

578 ibid.

579 *Senate FOI report*, op. cit., para 33.43-4 cited in Attorney-General's Department, *Submissions*, p. S403.

580 p. S403. See also Australian Customs Service, *Submissions*, p. S495 and New South Wales Law Society, *Submissions*, p. S860.

581 Attorney-General's Department, *Submissions*, p. S403.

582 ibid.

the amounts outstanding. The ATO also noted that community expectations concerning information provided in confidence to the ATO do not diminish with time.[583]

9.4.4 There are some circumstances where the relevant exemptions do not apply and disclosure of third party confidential information may be appropriate. For example, disclosure would be appropriate where the relevant third party consents to the release of the information.[584] The Attorney-General's Department suggested that in order to establish when release is appropriate, a system could be established whereby third parties indicate (at the time the information is collected) whether they wish data concerning them to remain confidential.[585]

9.4.5 It should also be noted that under the law on confidence, there are some situations where disclosure may be appropriate such as disclosure in the public interest (for example, where the information relates to an actual or contemplated wrong by the information supplier or where issues of public safety are involved.[586]) Disclosure will also be appropriate where secrecy provisions permit such disclosure – for example, where disclosure is allowed in the performance of an officer's duties under an enactment.

9.5 The appropriateness of provisions governing access

9.5.1 The view of the Attorney-General's Department is that the regimes established under the Archives Act and the FOI Act are generally appropriate in governing access to third party information.[587] Other submissions also considered the present provisions appropriate.[588]

9.5.2 The Committee concludes that, on the evidence presented, the provisions in the Archives Act which govern access to third party information are appropriate. It considers that the general rule allowing public access to archives after the 30 year period has elapsed, with categories of exempt records, is also appropriate. On the evidence received by the Committee, the provisions which govern access to third party information under

---

583 *Submissions*, p. S338. Note subsection 33(3) of the Archives Act in this context.

584 This is recognised in the Information Privacy Principles (see exception (b) to IPP 11.1) and by the general law on confidence. *Submissions*, p. S403.

585 *Submissions*, p. S403.

586 ibid.

587 ibid., p. S402.

588 See AFP, *Submissions*, p. S79 and DAS, *Submissions*, p. S728.

the FOI Act appear appropriate. However, the extensive review of the FOI Act currently being conducted by the ALRC and the ARC may examine this issue in greater detail.

9.6 Public register information

9.6.1 The Privacy Act regulates the handling of personal information held by Commonwealth agencies with a few exceptions.[589] 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.[590]

9.6.2 Advances in information technology allow this information to be searched, analysed and modified. As a consequence, public register information may be used for purposes which were not originally anticipated. For example, share register information is available to the public without restriction on payment of a fee. The register can be modified and used by direct marketers for commercial purposes.[591] Similar problems exist in relation to information on the electoral roll.

9.6.3 The Privacy Commissioner suggested that when public register information is modified, the new database should be subject to privacy safeguards. He commented that:

> Even though the information contained in it [the database] is, in another form, available to the public, the modified database is, for all practical purposes, a new record of personal information, which may be capable of uses which were impossible or impractical using the original public register.[592]

9.6.4 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 those for which the information was collected[593];

589 Privacy Commissioner, *Submissions*, p. S573.

590 ibid.

591 ibid.

592 ibid., p. S574.

593 ibid.

- where public register information is used for unintended 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[594]; 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.[595]

9.6.5 In light of the Privacy Commissioner's comments, the Committee considers that access to public registers and the possible uses of that information may need to be reviewed. It suggests that it may be appropriate for the Privacy Commissioner to coordinate a review of the reasons for allowing access to existing public registers, particularly where technology allows unintended uses of the information contained on the register. This review should also consider limiting access to registers or limiting the purposes for which public register information should be used.

> *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.

9.6.6 The Australian Electoral Commission (AEC) maintains a computerised data base which includes personal information on approximately 11 million Australian citizens.[596] On the enrolment form the information sought from citizens includes name, residential address, phone number, postal address, former surname, former address, occupation, gender, date of birth, town of birth, country of birth, whether the elector is an Australian citizen and if the elector is a citizen by naturalisation, the date of naturalisation and the citizenship number.[597] The information stored on the electoral roll computer data base

---

594 ibid.

595 ibid.

596 *Submissions*, p. S462.

597 ibid.

that is obtained from the enrolment form is name, former name, residential address, postal address, date of birth, gender and occupation.[598]

9.6.7 The names and addresses of all electors (except silent and itinerant electors) are publicly available on published electoral rolls which are printed on paper and in microfiche form. Members of the public can inspect or purchase the rolls in either format.[599] The Commission commented that:

> The publication of electoral rolls is an essential part of Australia's free and fair electoral process. It is a means of ensuring that participants in the electoral process are able to verify that elections are conducted honestly and without fraud. It allows everyone to know who is eligible to vote and permits the public to object to the enrolment of any elector.[600]

9.6.8 The Commission informed the Committee that only prescribed Commonwealth departments and authorities are supplied with gender, occupation and date of birth enrolment information (that is, non-public enrolment information).[601] Non-public enrolment information is only disclosed to prescribed agencies if the use to which the information will be put is sufficient justification for disclosure under Information Privacy Principle 11 of the Privacy Act. Generally, information is only disclosed in this way where disclosure is required or authorised by or under law, or where the disclosure is reasonably necessary for the enforcement of a criminal law or of a law imposing a pecuniary penalty or the protection of public revenue.[602]

9.6.9 Subsection 91(1) of the *Commonwealth Electoral Act 1918* deals with the provision of electoral rolls, supplements and habitation indexes to political parties, Senators, members of the House of Representatives and any other persons or organisations that the Electoral Commission considers appropriate. If a tape or disk is provided in this manner, subsection 91A(1) provides that the information must not be used other than for a permitted purpose. Furthermore, subsection 91B(2) provides that protected information must not be disclosed unless the disclosure would be a use of the information for a permitted purpose. The penalties for both offences are $1 000. (The permitted purposes vary slightly depending on the group or person to whom the rolls are provided, but include any purpose in connection with an election or referendum and monitoring the accuracy of information contained in the Roll.[603])

---

598 ibid.

599 ibid., p. S463. See also subsection 90(1) of the *Commonwealth Electoral Act 1918*.

600 ibid, p. S464.

601 See subsections 91(9), (10) and (11) of the Commonwealth Electoral Act.

602 AEC, *Submissions*, p. S469.

603 See subsections 91A(1A), 91A(2) and 91(2A) of the Commonwealth Electoral Act.

9.6.10 In its submissions the Commission identified two major problems in relation to access to electoral rolls; one of which has been remedied. The first problem related to a potential conflict between the Electoral Act and the FOI Act which resulted in potentially greater access to electoral information under the FOI Act than was available under the Commonwealth Electoral Act. The Commission informed the Committee that the insertion of a new category of exempt documents under the FOI Act in 1992 remedied this problem.[604]

9.6.11 The second problem identified by the Commission concerns the commercial use of electoral rolls. The Commission informed the Committee that technological advances have enabled commercial interests to have the electoral rolls scanned electronically and quickly duplicated into computer format.[605] As the microfiche is updated every six months, this provides very accurate personal information. Once in computer format the roll provides a means of data-matching and updating data bases to ensure address details are correct. This information, or extracts of it, is then sold. The data bases may ultimately be used for commercial purposes, such as direct marketing campaigns, or investigative purposes.[606] The Commission has informed the Committee that there is uncertainty as to whether it has copyright over electoral rolls. It noted that this fact, combined with the lack of on-use restrictions applying to published roll data, means that it is not possible to currently restrict commercial use of the Roll.[607]

9.6.12 The Commission cited some instances where electoral information has been used for commercial purposes. For example, in advertising a new data-matching program, a private company described its program as 'the latest in search technology with over 11 million entries compiled from the latest edition of the national electoral rolls'.[608] The Commission noted that it has received complaints from people objecting to their personal details being used for such purposes. The Commission is concerned that the use of the Roll for commercial purposes may discourage people from enrolling (which is an offence) on the basis that they do not want their personal details used by commercial enterprises.[609]

---

604 *Submissions*, pp. S740, S1055. Section 47A of the FOI Act provides that the following are exempt documents: a document that is an electoral roll, a print, microfiche, tape or disk of an electoral roll, a document used in preparation of an electoral roll, or a document derived from the electoral roll.

605 ibid., p. S466.

606 ibid.

607 ibid., p. S1056.

608 ibid.

609 ibid., p. S466.

9.6.13 The Commission submitted that a possible solution to the problem may be to introduce end use restrictions on data obtained from the Roll, similar to the restrictions under section 91A and 91B of the Commonwealth Electoral Act (outlined previously) which currently apply to the use of data provided on tape or disk.[610] These restrictions provide that data may only be used for permitted purposes. Permitted purposes, for a person or organisation *other than* a Senator, member of the House of Representatives or political party, are:

- any purpose in connection with an election or referendum;
- monitoring the accuracy of information contained in the Roll; and
- any other prescribed purpose. (The only purposes currently prescribed are for the conduct of medical research and the provision of public health screening programs[611]).

The proposal would result in the limitations currently placed on electoral data provided on tape and disk being imposed on electoral data available in hard copy and microfiche form.

9.6.14 Representatives from the Commission did, however, allude to the potential difficulties in policing and administering misuse of electoral roll data[612], even if this proposal were implemented.

9.6.15 The Committee agrees with the Commission's proposal to restrict end uses of all data derived from the electoral roll. The extension of end use restrictions to electoral data in hard copy and microfiche form appears logical. The Committee notes that imposing restrictions on the use and disclosure of electoral data regardless of its source will be difficult to enforce. However, it notes imposing such restrictions will be an improvement on the current situation. It may at least mean that companies will not advertise data-matching programs as containing entries compiled from the electoral rolls (as outlined at paragraph 9.6.12).

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.

610 ibid., p. S1056.

611 See paragraph 91A(2A)(c) of the Commonwealth Electoral Act and regulation 10 of the Electoral and Referendum Regulations 1993.

612 *Transcript*, pp. 373–374.

9.7 Access to medical records for statistical and research purposes

9.7.1 Access to third party information in the form of medical records was an issue which was brought to the Committee's attention. An individual's right to privacy in respect of her or his medical records is protected under the common law duty of confidence. However, medical records can be disclosed for epidemiological purposes without the consent of the person involved.

9.7.2 Epidemiology is the study of the distribution and determinants of disease. Epidemiological research is based on information about the health status of individuals and their exposure to factors that may affect their health.[613] Research methodology may involve the use of personally identifiable records of individuals, or non-identifiable (anonymous) data drawn from confidential records. Information is obtained from medical records and occupational or census records, and in some cases may also be obtained directly from the individual concerned.[614]

9.7.3 The Committee notes that epidemiological research has assisted in identifying a number of public health issues. Those issues include the increased risk of cancer associated with occupational exposure to certain substances, such as asbestos and vinyl chloride, and the increased risks of birth defects in children of women who become infected with German measles while pregnant.[615]

9.7.4 Subsection 95(1) of the Privacy Act provides that 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 guidelines apply to researchers and Institutional Ethics Committees (IECs) whose research involves the disclosure of personal information by a Commonwealth agency or the collection of personal information by a Commonwealth agency on behalf of the medical researcher. Prior to approving the issue of the guidelines, the Commissioner must be satisfied that the public interest in promoting the research outweighs, to a substantial degree, the public interest in adhering to the Information Privacy Principles.[616] For example, the provision of identifiable data to researchers without the consent of data subjects contravenes IPP 10.1(a) which requires consent to be obtained where data obtained for one purpose is used for another purpose.[617]

---

613 AIHW, *Transcript*, p. 608.

614 ibid., p. 610.

615 ibid., pp. 609–610.

616 Subsection 95(2) of the Privacy Act.

617 See Public Interest Advocacy Centre, *Submissions*, p. S1012.

9.7.5 The *Australian Institute of Health and Welfare Act 1987* allows the Institute to release identifiable data to external researchers with the agreement of its ethics committee.[618] The Privacy Commissioner has advised, and the Institute has accepted, that all relevant NHRMC guidelines be adhered to in respect of research using this type of data.[619]

9.7.6 The NHMRC Statement on Human Experimentation includes a supplementary note on Ethics in Epidemiological Research which provides:

> Consent of subjects should generally be obtained for the use of their records for medical research, but in certain circumstances an ethics committee may approve the granting of access to records without consent. This course should only be adopted if the procedures required to obtain consent are likely either to cause unnecessary anxiety or to prejudice the scientific value of the research and if, in the opinion of the ethics committee, it will not be to the disadvantage of the subjects.[620]

The Committee considers that, if at all possible, the consent of a data subject should be obtained before the subject's records are used in medical research.

a) Role of AIHW and IECs

9.7.7 The Australian Institute of Health and Welfare (AIHW) maintains a range of statistical collections for the purpose of health research.[621] The Australian Institute of Health Ethics Committee advises the Institute on the acceptability, on ethical grounds, of activities that are proposed or being undertaken by the Institute or other bodies in association with the Institute.[622] The Committee considers written information about professional and research activities brought to its attention. Institutional Ethics Committees also exist in research institutions, major hospitals and universities.

9.7.8 When activities are to be carried out by non-Institute personnel, the Ethics Committee insists that applications be made initially for clearance by local IECs. The AIH Ethics Committee then considers the proposal and encourages the relevant documentation from the local IEC's to be supplied to it.[623]

---

618 See paragraph 29(2)(c) of the AIHW Act.

619 AIHW, *Submissions*, p. S921.

620 See PIAC, *Submissions*, p. S1012.

621 AIHW, *Transcript*, p. 592.

622 See 'Policies and Procedures for Security and Confidentiality of Information held by the AIH in AIHW, *Submissions*, p. S95.

623 ibid., p. S95.

9.7.9 The AIHW maintains two registries, namely the Cancer Registry and the National Death Index. The Committee received evidence from the AIHW on the operation of the National Cancer Registry and the State cancer registries, and the extent to which patients are aware that identifiable data concerning them may be disclosed to external researchers.

9.7.10 Registration of cancer is mandatory in all States and Territories.[624] 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.[625] Individuals are advised that details of their medical condition may be collected pursuant to State legislation.[626] 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.

9.7.11 The AIHW is the custodian of the data from all State and Territory cancer registries for the purpose of producing national cancer statistics. The States and Territories retain ownership of the data and can control the use of their data or request its return.[627] Identifiable data is only released where the providers of the data (that is, the state cancer registries) give their consent.[628]

b) Options for consent/notification of possible uses of medical records

9.7.12 The Committee considered how patients could be most effectively informed about the use that may be made of their medical records.

(i) Requirement of consent

9.7.13 It was suggested that general practitioners could be required to obtain the written or verbal consent of the patient before sending the specimen on for cancer registration.[629] Dr Armstrong, Director of AIHW, noted that a consent requirement would produce serious biases, distort incidence data and make the data unreliable for

---

624 At the time of AIHW's submission, registration of cancer was not mandatory in the ACT (refer to p. S920). However, registration is now mandatory in all jurisdictions.

625 *Submissions*, p. S920.

626 ibid.

627 ibid.

628 *Transcript*, p. 606.

629 ibid., p. 600.

public health monitoring and cancer control purposes.[630] It was also noted that requiring consent would adversely impact on research and destroy the veracity of the statistics.[631]

9.7.14 Furthermore, if it was the responsibility of the doctor to give an assurance that the patient has consented to the data being passed on to a registry and if the doctor failed to raise the issue with the patient, then the doctor would be likely to take a 'null position' and to say that the patient had not given his or her permission.[632]

(ii) Notification

9.7.15 Notifying cancer patients of the possible use of medical records for cancer registration and research purposes is a second option. Dr Armstrong commented that notification would need to take place 'at the level of primary collection of the data'.[633] He appears to fully support the idea of notifying patients of the possible use of data concerning them for statistical and research purposes and he noted two ways of doing this. First, individual patients could be notified that information may be used for certain purposes (cancer registration and research). This notification could take place by dissemination of information at the point of hospital admission or in the doctor's surgery.[634] As a second measure, Dr Armstrong also suggested that the public could be informed about the register, its purpose and the type of information stored in it through a public education campaign.[635] The second measure could also be used to inform the public about the National Death Index.

9.7.16 If notification were a viable option, it would need to be built in to a routine administrative function.[636] As noted above, hospital patients could be informed about the use to which information may be put as part of admission procedures. In a general practitioner's surgery, the responsibility for notifying each patient of the purposes for which their medical records may be used would rest with the individual doctor.

9.7.17 While Dr Armstrong agreed that it may be possible to require doctors to notify patients about certain matters, he noted that this may be more problematic in a local doctor's surgery than a hospital. Where a doctor suspects cancer, he may not wish to

---

630 ibid., p. 616.
631 ibid.
632 ibid.
633 ibid., p. 593.
634 ibid., p. 594.
635 ibid., pp. 594, 597.
636 ibid., p. 594.

inform the patient that results of the biopsy may be passed on to the state cancer registry because that would immediately create some anxiety about the possible outcome of the diagnostic process.[637] Consequently, the doctor would need to adopt a general approach that did '. . . not have any particular implications for the diagnosis of the individual patient at the time that the information is provided.'[638]

9.7.18 The Public Interest Advocacy Centre (PIAC) supported the idea that medical practitioners be required to provide certain information to patients about cancer registries. The PIAC favoured statutory provisions imposing a duty on medical practitioners to provide the relevant information.[639] The PIAC also recommended that data subjects be informed that their records are kept on centralised State and Commonwealth cancer registries and informed as to how this information may be used.[640]

(iii) Removal of name from specimen

9.7.19 The Committee questioned the AIHW as to whether the name of the patient could be removed from the specimen[641] before it was forwarded to the registry so that the data would not be identifiable and confidentiality would be maintained. Dr Armstrong commented that removing names from specimens may create potential for double counting.[642]

9.7.20 If a practitioner takes a biopsy in his or her surgery and sends it to a pathologist, that information is forwarded to a cancer registry. If the biopsy reveals cancer, it may then be necessary to admit the patient to hospital for an operation. That information is also forwarded to the cancer registry. The patient may then be referred to a private radiotherapy clinic for treatment and that information may also be forwarded to the cancer registry.[643] If double counting occurs, it was argued that the cancer registry information '. . . will progressively degrade over time and become relatively useless as a means of monitoring the impact of cancer in the community'.[644]

---

637 ibid., p. 599.
638 ibid., p. 599.
639 *Submissions*, p. S1010.
640 ibid., p. S1011.
641 *Transcript*, p. 595.
642 ibid.
643 ibid.
644 ibid.

9.7.21 Personal identifiers are considered essential for collecting data on cancer patients for the following reasons:

- to eliminate multiple counting of a single tumour;
- to enable a tumour record to be completed with data obtained subsequently about recurrence, new primary cancers and death;
- to enable production of cancer survival statistics; and
- to provide information on past exposure to chemicals or other agents.[645]

The collection of identifiable data may also assist individuals in claiming compensation for exposure to chemicals.[646]

9.7.22 Researchers requiring access to a list of the names of people exposed to a chemical in a particular organisation and whether those individuals have had a cancer diagnosed can consult the National Cancer Registry. If that data is not available, the researcher would have to approach the various state organisations to get the same information.[647] Furthermore, to be able to compute survival rates (after diagnosis of cancer), researchers need to be able to link the names of the people with cancer to the names of those who have died.[648]

9.7.23 The PIAC was attracted to a system of unique identifiers and suggested that the Privacy Commissioner be asked to investigate whether European systems which use pseudonymous identifiers pose an impediment to research.[649]

(iv) Comments

9.7.24 The Committee considers that individuals should be made aware that details of their condition may be forwarded 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 hospital admissions department) verbally informing the patient that details will be forwarded to the relevant registry, the Institute and may ultimately be used for research purposes.

9.7.25 The Committee further considers that cancer patients should be informed in writing that details will be forwarded to the registry, the Institute and may be used for research. This written notification should be forwarded within a week of the verbal

---

645 ibid., p. 616

646 ibid., pp. 600–601.

647 ibid.

648 ibid.

649 *Submissions*, p. S1009.

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.

9.7.26 The Committee acknowledges that it may be difficult to ensure all primary collectors notify patients that information may be passed on to the cancer registry and researchers. Even if the requirement to inform was made mandatory, Dr Armstrong suggested that there may not be any way of ensuring notification actually occurred.[650] The Committee considers that measures designed to implement a national standard in this area may alleviate some of these difficulties.

9.7.27 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.

9.7.28 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. This recommendation applies to both the National Cancer Registry and the National Death Index.

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 conditions may be forwarded to cancer registries, the Australian Institute of Health and Welfare and may be released to external researchers.

650 ibid., p. 598.

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.

9.7.29 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 in addition to that for which it was collected, measures for notifying individuals of these practices should also be explored. Public education campaigns would also be useful in this respect.

Chapter 10

The need for a national privacy code

This chapter addresses a proposal which was not directly the subject of the terms of reference for this inquiry but which should not be avoided in a study of the Commonwealth's protection of confidential third party information. The proposal for a national privacy code arises for many reasons. Information collected by the Commonwealth is not necessarily held only by the Commonwealth. Further, technological advances permit information collected by the Commonwealth to be accessed and manipulated by the non-government sector in increasingly sophisticated ways. There have also been significant changes to the public sector through privatisation and contracting out of services, which affect the scope of the Privacy Act in relation to functions which were previously the preserve of government. Differential privacy standards are arising within the private sector and these may have adverse implications for Australian companies seeking to sell goods and services in the international market.

10.1 The scope of privacy protections

10.1.1 The Privacy Act has been criticised on the grounds of its limited jurisdictional scope. As discussed above, the Privacy Act applies only to the Commonwealth Government and its agencies, except where specifically excluded. It does not apply to the private sector other than to credit reporting organisations. Nor does it apply to state or territory governments.

10.1.2 The Committee is aware that almost on a daily basis, there are very public examples of disregard for privacy concerns, sometimes concerning information collected by the Commonwealth. A recent matter involved Comcare material printed from a stolen portable computer. A public disclosure was effected when an unknown party gave material produced from the stolen computer to the CPSU who then offered it to the media to view. The Committee recognises that the CPSU was not responsible for the initial disclosure by theft, but it has some sympathy for the lament of Comcare that '[t]he CPSU, however, released the information to the press and other third parties which in our view, constitutes a breach of privacy principles.'[651]

10.1.3 An initial unauthorised disclosure should not entitle others to deal with confidential information as they choose. In this case, one breach of privacy was compounded by another. Clearly the Privacy Act does not extend to the protection of

651 Comcare, *Submissions*, p. S1083.

material released by this sort of chain reaction, but it is reasonable to question whether such confidential information should be completely without protection.

10.1.4 Another important factor in deciding to consider limitations on the scope of the Privacy Act in this report is the recognition by the Committee that information often does not exist in separate and discrete holdings. Technological advances, especially digitalised information, means that information collected by the Commonwealth may not remain the exclusive preserve of the collecting agency. It may be transferred to or accessed by other government agencies or the private sector. Information may have been provided for a purpose such as registering on the electoral roll, but private sector organisations may access that information and use it for a purpose which was not contemplated by the provider when the information was provided.

10.1.5 A guiding principle when dealing with confidential third party information should be that, confidential information provided to an agency for one purpose should not generally be used by other agencies or for unrelated purposes, unless such use is expressly authorised. This is currently unenforceable. There are many opportunities for authorisation to be given for confidential third party information held by the Commonwealth to find its way into the hands of an agency that is non-Commonwealth. It would be short sighted not to consider the possibility of privacy protections having a broader scope than those currently provided for under the Privacy Act.

10.2 Existing privacy protections in the non-Commonwealth sphere

10.2.1 Privacy codes already exist within the non-Commonwealth sphere of operations. One example is *The Australian Privacy Charter.* It was issued in December 1994 by the Australian Privacy Charter Council, chaired by the Hon Justice Michael Kirby.[652]

10.2.2 The Australian Direct Marketers Association (ADMA) has codes of practice which apply in part to the privacy aspects of the activities of private sector agencies.[653] The ADMA has made suggestions about the possible use of those codes to an inquiry into privacy and other issues relating to direct marketing, being conducted by Working Group on Direct Marketing of the Standing Committee of Officials of Consumer Affairs. The ADMA has suggested that it develop a policy position on all aspects of privacy and data protection as they relate to direct marketing, including up-dating and revising codes

652 Greenleaf G., 'Information Technology and the Law', 69 ALJ 90.

653 Australian Direct Marketing Association Ltd, *ADMA response to SCOCA Working Group on Direct Marketing discussion paper*, May 1995.

of conduct. The ADMA argued further that following its revision the codes of conduct should be scheduled under state and territory fair trading legislation thus giving them wide currency throughout Australia.

10.2.3 The Privacy Commissioner has commented that ADMA's standards while worthwhile, are insufficient because they do not address a number of important privacy principles and as a self-regulatory measure, there is a lack of redress for consumers.[654]

10.3 Calls for national privacy protection

10.3.1 The Committee is aware that the limited scope of the Privacy Act has been considered on many occasions and that the Government has not chosen to extend either the scope of the Act or the extension of protection of confidential information by some other scheme. While this matter is complementary to the current terms of reference rather than an integral part of them, the Committee considers this inquiry offers a convenient opportunity to canvass the issue.

10.3.2 The Privacy Commissioner believes that the scope of the Privacy Act is too narrow even within the Commonwealth sphere. Concerns about the coverage of the Act were expressed in his 1989–90 Annual Report and these were considered by the Senate Legal and Constitutional Affairs Committee.[655] The Government response to the report rejected the recommendation that the coverage of the Privacy Act be extended (to encompass sanctions against offending public servants and remedies for persons suffering harm from unauthorised disclosure) in the following terms:

> The main reason is that such amendments would not be consistent with the essential role of the Privacy Commissioner, which is to oversee the collection, handling, use and disclosure of personal information by Commonwealth *agencies*.[656]

10.3.3 The Privacy Commissioner has proposed that a national privacy policy would be the best means of enhancing protection of an individual's personal data, regardless of whether she or he was dealing with the private or public sector.[657] This proposal is based on three premises. The first is that there is a proliferation of privacy codes in

---

654 Ministerial Council on Consumer Affairs, *Report of the Working Party on the sale of mailing lists*, July 1994, p. 72.

655 *Unauthorised Procurement and Disclosure of Information*, June 1991.

656 Government response to ibid., p. 2.

657 Privacy Commissioner, *Submissions*, p. S1068.

different sectors of the community. The second is that the information superhighway presents significant new policy challenges. The third is the continuing trend towards greater information sharing between state and Commonwealth governments and the consequent movement of information collected or held under the Commonwealth privacy regime, to the largely unregulated state sphere. The Privacy Commissioner commented that:

> [t]his raises questions about the potential for inappropriate re-use of information which was collected for a particular purpose, security and difficulties of redress for individuals who believe that their information has been mishandled.[658]

10.3.4 There is overseas opinion to support the proposals for a national code. The Council of Ministers of the European Parliament formally adopted a common position on a directive on the protection of personal data on 21 February 1995.[659] The directive is aimed at ensuring a high level of protection for the privacy of individuals in member states. Importantly, Single Market Commissioner Mario Monti commented that the directive would provide major advantages for business:

> . . . particularly as it constitutes an essential element for the free flow of services in the Information Society by fostering consumer confidence. And besides the development of these new markets, business competitiveness stands to gain considerably from the efficiency gains made possible by the application of these services.

10.3.5 The significance of the information superhighway is an issue that was expressly considered by the European Union in the formulation of its protections for personal data. Comments about the difficulties associated with separate protection regimes, by the European Union are relevant to all countries seeking to pursue business in the international market place, including Australia:

> If each Member State had its own set of rules on data protection, for example on how data subjects could verify the information held on them, cross-border provision of services, notably over the information superhighways, would be virtually impossible and this extremely valuable new market opportunity would be lost.[660]

---

658 Privacy Commissioner, *Submissions*, p. S1068.

659 Delegation of the European Commission to Australia and New Zealand, *Council adopts common position on protection of personal data directive*, 21 February 1995.

660 Delegation of the European Commission to Australia and New Zealand, *Council adopts common position on protection of personal data directive*, 21 February 1995, p. 1.

10.3.6 Dr June Factor, a member both of the Privacy Advisory Committee and of the Victorian Council for Civil Liberties, also spoke strongly in favour of the need for a national code:

> One of the firm convictions that I have gained from my couple of years on the Privacy Advisory Committee is that there needs to be legislation that covers the States, just as there needs to be legislation that covers private bodies as well as government instrumentalities.[661]

10.3.7 Dr Gordon Hughes is a solicitor with expertise in data protection. He told the Committee that the structure of the Privacy Act, while suitable, was limited because the obligations and controls it contained did not extend to the private sector. He considered it to be '. . . very much a half way house to control Commonwealth departments and not to control the private sector, where I am sure the serious breaches occur.'[662]

10.3.8 Professor Gregory Tucker, an academic lawyer who has expertise in information privacy law, also argued that privacy legislation should extend to the private sector:

> I believe the area should be covered by all-embracing legislation; it does not necessarily mean draconian measures. It seems appropriate across an information market that the same standards be applied as appropriate. That is a national issue rather than a state by state or territory issue. It seems to me there is enough international connection that it may be constitutionally possible to provide for a national law in this area.[663]

10.3.9 The Privacy Commissioner summed up his position on the issue with this proposal:

> I consider that it is timely to review the scope of the Privacy Act with a view to extending its coverage to include state and territory agencies and the private sector to ensure a consistent level of protection to the individual's human rights irrespective of whether that individual deals with a state or Commonwealth agency or the private sector.[664]

10.3.10 The Committee agrees that it is desirable to have uniform standards of protection for privacy which would apply on a consistent basis to confidential personal information in all circumstances. The Committee notes that even in the Commonwealth sphere the coverage of the Privacy Act is being weakened by the increasing tendency to contract out services which in the past were performed within an agency, and by privatisation. Services which were once the exclusive preserve of government are now

---

661 Dr J. Factor, *Transcript*, p. 134.

662 Dr G. Hughes, *Transcript*, p. 413.

663 Professor G. Tucker, *Transcript*, pp. 446–447.

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

being provided by the private sector or by semi-governmental enterprises which are not covered by the Privacy Act. This is a matter of some concern as the services already privatised or being considered for privatisation include sensitive areas with almost blanket coverage of the population such as telecommunications, electricity and water supply. Telecom provides an instructive illustration of the relevant issues.

10.4 Telecom and privacy protection

10.4.1 Telecom (Telstra from July 1995) made four submissions to the inquiry and gave oral evidence on two occasions.[665] The Australian and Overseas Telecommunications Corporation (Telecom) ceased to be an 'Agency' as defined in the Privacy Act in February 1992,[666] in order that it might compete with other providers which were not subject to the Act. It is therefore no longer subject to the Privacy Act except in relation to tax file numbers and credit reporting.[667]

10.4.2 Telecom exemplifies the issues relevant to the protection of confidential third party information held by agencies not subject to the Privacy Act. As noted above, it is one of those organisations which provide services which were once a government monopoly. It holds huge quantities of information about individuals and businesses, much of which was collected when the organisation was a Commonwealth agency. It has sophisticated technology which permits the access to and manipulation of the data by the organisation itself. In addition the information held by Telecom is subject to access and manipulation by other organisations with equally advanced technology. It is one of many agencies outside the protection of the Privacy Act which implements its own privacy codes. Indeed the organisation has adopted the Information Privacy Principles as policy in relation to its information handling activities.[668] Telecom has also been the subject of very well publicised lapses in its handling of confidential third party information.

10.4.3 The circumstances of Telecom's difficulties in protecting the confidential information of its clients, raise questions about whether the Commonwealth should continue to limit its role in this area to the agencies currently covered by the Privacy Act. In response to matters raised by the New South Wales ICAC[669], Telecom instituted a

---

665 Submissions 12, 23, 83 and 99. Telecom representatives appeared before the Committee on 21 October 1992 and 21 September 1993.

666 *Submissions*, p. S162.

667 *Evidence*, p. 429. Telecom is also referred to in Appendix E in the context of a case study of agencies referred to by the New South Wales ICAC.

668 ibid.

669 See Appendix E of this report.

Code of Conduct in May 1993. In September 1993 the organisation appeared for the second time before the Committee and reported

> ... we have examined other security aspects of our systems and we have in place a series of processes, some fully developed and about to be implemented such as centralisation of certain staff, and some still in the systems development and appreciation phase, that will remove the environment that we believe allowed the ICAC cases to occur in New South Wales. I think that gives us, certainly in Telecom, a degree of assurance.[670]

10.4.4 The organisation was optimistic that it was coping with the considerable task of protecting such a large amount of confidential information but noted that it was not a finite task:

> ... I really do not believe that with the technologies we are using – both IT technologies and perhaps more standard communication technologies – the job of ensuring adequate security of information is ever finished. ... That is why we have a fairly large group of system security people who are almost guaranteed lifetime employment, so long as their skills remain current.[671]

10.4.5 This qualification appeared to demonstrate that Telecom management appreciated the dimensions of its task and was making every effort to meet its obligations. This evidence was being given at the time Telecom was under serious strain over its legal liabilities to clients who had suffered commercial loss because of the alleged failure of Telecom services – the so-called COT (Casualties of Telecom) cases. The publicity surrounding the cases was an additional stress. On 2 September 1993 Telecom told a Senate Estimates Committee that it had paid compensation to some complainants although the organisation denied legal liability. Telecom assured the Estimates Committee that it was dealing with its client problems in an appropriate way.[672]

10.4.6 The 7.30 Report on 7 February 1994 revealed that Telecom was in fact monitoring, in a systematic way, the telephone calls of several COT complainants. One customer had all her calls recorded for nine days.[673] At the same time Telecom management was assuring both the Senate Estimates Committee and this Committee that it was dealing with the whole area of privacy in a proper manner. Since these revelations there has been a great deal of activity aimed at saving Telecom from a further erosion

---

670 *Evidence*, p. 422.

671 ibid., p. 424.

672 The 7.30 Report on 7 February 1994 quoted Telecom at the Estimates Committee of 2 September 1993 as saying "We don't believe that there are systemic and repetitive faults. If faults have been detected, they've been dealt with..." (Transcript of 7.30 Report, Department of the Parliamentary Library).

673 ibid.

of public confidence in its integrity. In advertising for a privacy auditor the organisation stated 'Telecom is fully committed to the protection of personal privacy...'[674]

10.4.7 Despite the fact that the telecommunications industry has structures in place which address privacy issues[675], the Committee considers that the capacity of the industry to have an adverse impact on the privacy of its clients remains of great concern. The Committee considers that a national privacy code would assist in bringing a consistent standard of protection to confidential third party information in the telecommunications industry. The code would complement, rather than replace the structures already in place in the telecommunications industry.

10.5 Privacy protection, government business enterprises and self regulation

10.5.1 Of course the Privacy Act or parts of it could be extended on a fractional basis to expressly targeted operations and activities of government business enterprises. It seems to the Committee to be a partial solution only and therefore unsatisfactory. It is also one that might unduly increase the administrative complexity of the agency or business concerned.

10.5.2 In the context of the Committee's discussion on the increasing tendency for agencies to contract out functions that involve the use and transfer of sensitive third party information, the Committee proposed a single focussed solution of extending liability for observance of the Information Privacy Principles to contractors.[676] Another solution would be to extend a privacy regime to all spheres of activity.

10.5.3 In relation to the privatisation of Commonwealth Government functions the Committee considers that it is desirable to protect third party information that becomes part of private sector held information. This includes information that may have been obtained when the Privacy Act applied to the agency holding that information, but which is no longer subject to those safeguards because the agency itself is no longer subject to the Privacy Act. In such cases there is often a measure of self regulation which connects the new enterprise with its previous obligations under the Privacy Act. The Telecommunications Industry Ombudsman (TIO) Scheme is an example.

---

674 *The Age*, 27 August 1994.

675 These include the Telecommunications Industry Ombudsman, Austel's Privacy Advisory Committee and Telecom's privacy auditor.

676 Refer to chapter 3.

10.5.4 The TIO Scheme has been established to provide independent resolution of complaints and disputes regarding telecommunications services.[677] The protection offered by the TIO covers:

> interference with the privacy of an individual in terms of non-compliance with the Information Privacy Principles contained in s. 14 of the Privacy Act 1988 or any industry specific privacy standards which may apply from time to time.

10.5.5 The TIO has powers similar to those of the Privacy Commissioner, to investigate a complaint and to resolve it by:

> i) making a determination that the participant, the subject of investigation, pay compensation to a complainant; . . .
> v) directing a participant to include or omit an entry in any electronic or printed directory; . . .
> vii) directing a participant to make an appropriate correction, deletion or addition to a record; . . .
> ix) directing a participant to do, not to do, or to cease doing, an act;
>
> provided that the total of such determinations or directions in relation to an individual complaint are not to exceed in value $10,000 . . . .

10.5.6 There is also an important linkage between the TIO and the Privacy Commissioner, as both are members of the AUSTEL Privacy Advisory Committee which was established in 1994. While the Committee supports the TIO Scheme and other self regulatory schemes as worthwhile measures in protecting privacy, a disadvantage is that a multiplicity of schemes results in inconsistencies in privacy protections for individuals and businesses.

10.5.7 The Administrative Review Council (ARC) has recently reported on *Government Business Enterprises and Commonwealth Administrative Law*.[678] The Committee agrees with the ARC's comments that the political context for Government Business Enterprises (GBEs) and Commonwealth agencies is 'the fulfilment of government objectives and the fulfilment of the community's expectation in GBEs maintaining the highest possible social and ethical standards.' The community has the right to expect a high standard from government agencies, including those engaged in commercial activities.

---

677 Telecommunications Industry Ombudsman, *Jurisdiction* (pamphlet).

678 Administrative Review Council, *Government Business Enterprises and Commonwealth Administrative Law* (Report No. 38) 1995 Canberra, A.R. McLean Printing.

10.5.8 It is fundamental that the confidential nature of information which derives from third parties is just as confidential regardless of the commercial or non-commercial nature of the holders' activities. Disclosure per se affects the privacy of the third parties who provide the information and who are the subject of that information. The Committee notes the ARC's position that exclusion from the ambit of the Archives Act is not to be justified on the basis that a body undertakes commercial activities[679]. The Committee considers that commercial activity is no reason to withdraw protection for confidential third party information. Accordingly, the Committee strongly supports the extension of privacy protection to government business enterprises by way of a national privacy code for Australia.

10.6 Privacy protection and the non-government sector

10.6.1 The desirability of consistent protection for confidential third party information is applicable also to the non-government (private) sector. The benefits would extend beyond the individuals and businesses desiring the confidentiality, to the private sector holders of the information. The Committee considers that there will be advantages to the private sector in having consistent standards for the protection of privacy rather than several or more sets of rules on the protection of confidential information.

10.6.2 For any transnational operations between agencies in Australia and European Union countries a national code of privacy providing a high level of privacy protection will enable Australian agencies to conduct their activities in a reasonably free way, without the need to refer to another layer of protections.

10.6.3 The *Report of the Working Party on the sale of mailing lists* to the Ministerial Council on Consumer Affairs notes the comment of the NSW Privacy Committee that:

> . . . in the absence of adequate data protection controls, it is likely that Australian governments and businesses which wish to receive data from, or transfer data to, European Community members will be required to enter into contracts to guarantee the privacy rights of data subjects.[680]

679 ARC, *Government Business Enterprises and Commonwealth Administrative Law*, p. 44.

680 Ministerial Council on Consumer Affairs, *Report of the Working Party on the sale of mailing lists*, July 1994, p. 11.

10.6.4 That report also notes the implications of such a requirement have been taken very seriously indeed by two of Australia's closest neighbours, New Zealand and Hong Kong.

10.6.5 The New Zealand Privacy Act 1993 establishes a series of Information Privacy Principles which like the Australian Privacy Act draw on the OECD data protection principles.[681] The principles set out rules regarding the purpose, source, manner, security and storage, correction and accuracy of personal information. The significant difference between the two Acts is that the New Zealand Act applies to both the public and private sectors. The Act also places some controls on the administration of public registers. It prohibits the combining of information from separate public registers for the purpose of selling that combined information. Importantly, another feature is that a Complaints Review Tribunal has the power to make orders prohibiting repetition of breaches or requiring interferences with privacy to be put right. It can also require damages or compensation to be paid.

10.7 Constitutional basis for extending Commonwealth oversight of the protection of confidential information

10.7.1 The Committee considered it appropriate to seek advice on the constitutional position of the Commonwealth in extending its role in the protection of confidential third party information, including possible extension of the Privacy Act. The Attorney-General's Department has provided advice to the Committee in response to the question: 'Would the Commonwealth Parliament have power to apply information privacy laws generally in the private sector and also in the State and Territory public sectors?'

10.7.2 In summary, the advice was that the Commonwealth could rely on the plenary power to make laws for the territories under section 122, and that there was 'considerable scope' for privacy protection legislation for the states under the corporations power in

---

681 Ministerial Council on Consumer Affairs, *Report of the Working Party on the sale of mailing lists*, July 1994, p. 48.
The long title of the *Privacy Act 1993* (New Zealand) begins 'An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Cooperation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, and, in particular, –
(a) To establish certain principles with respect to –
(i) The collection, use, and disclosure, by public and **private sector agencies**, of information relating to individuals; and ...' (bold added)

section 51 (xx) of the Constitution. However, comprehensive legislation would have to depend upon the external affairs power in section 51 (xxix) of the Constitution.

10.7.3 The *Tasmanian Dams Case* is an authority for the Commonwealth to enact legislation under the external affairs power to give effect to international obligations.[682] Australia ratified the International Covenant on Civil and Political Rights (ICCPR) on 12 August 1980 subject to a number of reservations and declarations. Article 17 of the ICCPR provides:

> 1. No-one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to protection of the law against such interference or attacks.[683]

10.7.4 The advice concludes that on the authority of the *Tasmanian Dams Case*, the Commonwealth Parliament could enact legislation giving a right to privacy with exceptions in the cases of 'reasonable' interferences. The scope of the permissible exceptions would probably extend to interferences of the kinds now covered by the various exemptions in Information Privacy Principles 10 and 11 in section 14 of the Privacy Act.[684] The Committee notes the advice of the Attorney-General's Department on the issue of Constitutional power for the enactment of information privacy laws of general application in Australia. The Committee does not however seek to determine which head of law making power the government should rely upon in proposing legislation should that means of extending protection be endorsed. The Committee recognises the possibility that complementary state legislation may also be appropriate.

10.8 Conclusions

10.8.1 The Committee considers 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. The Committee notes that if such a code is effected by way of extension of the Privacy Act, consequent changes to the FOI Act would be necessary.

---

682 *The Commonwealth* v *Tasmania* (1983) 158 CLR 1.

683 Attorney-General's Department, *Submissions*, pp. S1019–S1020.

684 Attorney-General's Department, *Submissions*, p. S1021.

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.

10.8.2 As this proposal would have wide coverage in the Australian community, including application in state and territory government operations, the Committee considers 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.

Chapter 11

Afterword

11.1 Introduction

11.1.1 Since the Committee concluded its evidence taking, several matters have arisen which relate to the issues raised in this inquiry. The Committee learnt about these matters largely through media reports and matters being raised in parliament. Although it has not taken formal evidence, the Committee considers that it would be useful for it to comment on these matters in the context of this inquiry because they are illustrative of the problems identified within this report.

11.2 A weak privacy ethos in Commonwealth agencies

11.2.1 A matter discussed recently in the context of a Senate Estimates Committee hearing and involving the release of information about persons who have been exposed to the risk of Creutzfeldt-Jakob Disease, illustrates continuing weaknesses in the privacy ethos in some Commonwealth agencies. In May 1995 it was revealed that officers in the Department of Human Services and Health had released, without consent, personal information about pituitary hormone recipients to over thirty blood, organ and tissue banks. Dr Stephen Duckett, Secretary of the Department of Human Services and Health, made the following statement to a Senate Estimates Committee hearing:

> I think this is raising an issue of whether there should have been contact with these people before their personal information was released to other agencies, and I think what is of concern in this particular case is that, unlike the case where we are releasing personal information because we think people are doing nasty things, fraud and the like, these were people who we should be working with and should be assisting. I think it is raising an issue about whether I should issue guidelines throughout the department across all programs about release of personal information in this sort of case. I believe it is an area where I should issue such guidelines and will be doing that.[685]

11.2.2 The Committee notes with some concern that this incident is happening at a time when the Privacy Act has been on the statute books for seven years. It is disappointing to learn that only now is the head of the department thinking about issuing guidelines to

685 Australia, Senate, *Estimates*, 26 May 1995, proof issue, at p. CA 87.

staff about the release of personal information in this sort of case. It is also disappointing to learn that the department had no formal system for notifying persons involved at a time before or when it notified the blood, organ and tissue banks.

11.2.3 The Committee considers that this incident is indicative of the lack of an effective privacy ethos in the agency. It also demonstrates certain failings of the agency's senior managers, who as well as having responsibility for the direction and operations of an agency have a guiding role in influencing the ethos of an agency. In the extremely sensitive health area senior managers had neither implemented the systems to satisfy privacy concerns nor provided satisfactory direction and training to officers in regard to privacy matters.

11.3 Unauthorised disclosure of computer held information

11.3.1 A recent matter involving the unauthorised disclosure of confidential information taken from a departmental computer system illustrates several of the concerns raised in this report. An officer of the Attorney-General's Department disclosed, without authorisation, dozens of computer discs containing information taken from the computer system in the Attorney-General's Department.

11.3.2 It is not clear whether the information included confidential personal and commercial information. As the intention of the Attorney-General's Department officer concerned was to deliberately and wrongfully release confidential information, this case can be distinguished from those cases discussed above where officers acted deliberately but in ignorance of the wrongfulness of their actions and did not seek public release of the information disclosed. The implication from this case is not just that the privacy ethos is weak although this may also be a factor influencing the given behaviour. Privacy ethos aside, if an individual officer sets out deliberately to act in an unauthorised manner something more than improvements in the agency's privacy culture are required to protect confidential third party information. Other issues become critical.

11.4 Information technology security

11.4.1 Computer systems are a considerable aid to government administration however, they also represent a considerable threat to administration when they are inadequately managed. In the case mentioned above the offending officer stated that he had acted as he did in part to demonstrate how easy it would be to effect a widespread unauthorised

release of information onto the Internet communications system. Clearly the Internet presents an opportunity for widespread unauthorised disclosure of confidential information of any kind. The Committee notes that the expansion of access to the Internet is a matter of increasing significance in Australia and that it could be misused with potentially devastating effects on individual privacy.

11.4.2 An agency's security system for protecting computer based information should be designed to cope with all foreseeable threats. But not all risks can be foreseen. Precautions must be taken to detect those breaches which cannot be prevented. Security systems for computers need to be in place and need to be fully active. Senior managers need to take responsibility for the information technology security systems of their agencies and update them as the technology itself is updated. Systems standards should aim to prevent unauthorised disclosure. As a minimum, all agency security systems should be able to audit and identify wrongful access (and possible disclosure) and random 'audit trails' should be implemented. The frequency of testing the adequacy of an agency's security system should be a function of the amount of confidential information held and the sensitivity of the information.

11.4.3 An Audit Report on the Australian Bureau of Statistics[686] noted that 80 per cent of known computer abuse is from an organisation's own staff. Perimeter security and the requirement for all staff to sign a secrecy undertaking under the terms of the *Census and Statistics Act 1905* were

> not of themselves an effective control against the abuse of privileged access to information'. Good monitoring controls and audit trails of activity are essential to allow the detection of computer abuse.[687]

11.5 Administrative and criminal sanctions as a deterrent

11.5.1 Implementation of information technology security systems must be complemented by the enforcement of standards of conduct. Not only do the administrative and criminal sanctions for deliberate wrongful disclosure of confidential information need to be in place, after the wrongful disclosure is detected, they need to be used as a deterrent to other similar potential law breakers.[688]

---

686 *Audit Report No. 2, 1993-4 Australian Bureau of Statistics Computer Security,* Canberra 1993.

687 ibid., pp. xi–xii.

688 In relation to this observation the Committee notes that the offender in the recent Attorney-General's Department case received a nine months custodial sentence.

11.5.2 Another computer based issue which can have a broad impact on the lives of Australians is computer matching of confidential third party information by the private sector.

11.6 Computer matching by the private sector

11.6.1 In recent months there has been a renewed impetus for scrutiny of activities by the private sector in the area of data-matching. The widespread use of affinity purchasing programs – such as Fly Buys – exposes individuals to the likelihood of having their purchases of certain products or payments by a particular method, being included on separate computer data banks. This information can be manipulated by computer to reveal individual spending patterns or profiles. This practise is becoming increasingly sophisticated with the wider application of digitalised information. The information is used to enable direct marketers to target individuals for particular goods or services.

11.6.2 There is scope in some cases for an individual to instruct a retailer not to include her or his details in such a scheme, although opting out can be difficult. Not only is the personal information of an individual used in ways not necessarily contemplated at the time of purchasing, but the targeting could be considered by individuals to be intrusive. The Committee notes that a considerable amount of work has been done in the area of privacy issues and direct marketing in the context of the Standing Committee of Ministers for Consumer Affairs. The Australian Direct Marketing Association has provided the Committee with its submission to the Consumer Affairs inquiry and there is evidence that the industry itself accepts that some form of regulation is desirable.[689]

11.7 Conclusions

11.7.1 There are deficiencies in the approach to privacy for confidential information. There are also deficiencies in the approach to information technology security. The Committee considers that these deficiencies raise two significant issues. One is the lack of a genuine privacy ethos throughout the public sector, and the other is the lack of recognition of the technology dynamic in government administration. These inadequacies are indicative of the apparent failure of senior managers to deal satisfactorily with these issues.

---

689 The Association has developed a voluntary code of conduct which addresses the protection of privacy. It proposes that the code be the basis of a uniform code of conduct for the direct marketing industry.

11.7.2 There is a demonstrated need for senior managers to be responsible for the protection of confidential information. There is also a demonstrated need for a comprehensive and consistent approach to sanctions which can be applied to persons who are involved with unauthorised disclosures of confidential information.

Daryl Melham MP
Chair

June 1995

APPENDIX A

List of Submissions

Submission Number	Individual/Organisation
1	Mr B W Hamilton JP
2	A J Bayley
3	Queensland Law Society Inc
4	Ms Christine Heal
5	Merit Protection and Review Agency
6	Commonwealth Director of Public Prosecutions
7	Mr C Wilson
8	The Hon Adrian Roden QC
9	GIO Australia Ltd
10	Australian Library and Information Association
11	Confidential Submission
12	Australian Telecommunications Authority (AUSTEL)
13	Mr Charles Pitt
14	Australian Federal Police
15	Australian Anti-Bases Campaign Coalition
16	Australian Institute of Health and Welfare
17	Australian Society of Archivists Incorporated
18	Institute of Mercantile Agents Ltd
19	Ms Sue McKemmish Monash University
20	The Hon Alan Griffiths MP Minister for Tourism
21	Australian National Audit Office
22	Victorian Council for Civil Liberties
23	Australian and Overseas Telecommunications Corporation (AOTC) now trading as Telstra Corporation Ltd
24	Health Insurance Commission

25	Australian Transaction Reports and Analysis Centre
26	Australian Security Intelligence Organisation
27	The Hon Robert Tickner MP Minister for Aboriginal and Torres Strait Islander Affairs
28	Mr Peter Hallam
29	Business Council of Australia
30	Australian Postal Corporation
31	National Crime Authority
32	The Hon Gerry Hand MP Minister for Immigration, Local Government and Ethnic Affairs
33	Australian Archives
34	Australian Taxation Office
35	Attorney-General's Department
36	Department of Social Security
37	Australian Electoral Commission
38	Australian Customs Service
39	Public Service Commission
40	The Hon Adrian Roden QC **(Supplementary Submission to No. 8)**
41	Law Reform Commission of Victoria
42	Privacy Commissioner
43	Australian Press Council
44	Australian Securities Commission
45	Department of Health, Housing and Community Services
46	Department of Veterans' Affairs
47	The Hon Gordon Bilney MP Minister for Defence, Science and Personnel
48	Confidential Submission
49	Queensland Health
50	Confidential Submission
51	Department of Industrial Relations
52	Australian Security Intelligence Organisation **(Supplementary Submission to No. 26)**
53	Department of Finance

54	The Hon Leo McLeay MP Speaker of the House of Representatives
55	Department of Administrative Services
56	Mr Christopher Mann
57	Australian Electoral Commission **(Supplementary Submission to No. 37)**
58	Lakos & Company Solicitors
59	Queensland Law Reform Society Inc
60	New South Wales Privacy Committee
61	Australian Trade Commission
62	Professor Greg Tucker Monash University
63	Victorian Council for Civil Liberties **(Supplementary Submission to No. 22)**
64	Australian Postal Corporation **(Supplementary Submission to No. 30)**
65	Department of Defence **(Supplementary Submission to No. 47)**
66	Mr Christopher Mann **(Supplementary Submission to No. 56)**
67	Australian Bankers' Association
68	Health Insurance Commission **(Supplementary Submission to No. 24)**
69	Confidential Submission
70	The Hon Michael Lee MP Minister for Tourism **(Supplementary Submission to No. 20)**
71	The Hon Robert Tickner MP Minister for Aboriginal and Torres Strait Islander Affairs **(Supplementary Submission to No. 27)**
72	The Hon Laurie Brereton MP Minister for Industrial Relations **(Supplementary Submission to No. 51)**
73	Department of Social Security **(Supplementary Submission to No. 36)**
74	Confidential Submission
75	Law Institute of Victoria

76	Attorney-General's Department **(Supplementary Submission to No. 35)**
77	The Law Society of New South Wales
78	Confidential Submission
79	Public Interest Advocacy Centre
80	Ministry of the Premier and Cabinet Western Australia
81	Senator the Hon Nick Bolkus Minister for Immigration and Ethnic Affairs **(Supplementary Submission to No. 32)**
82	Australian Institute of Health and Welfare **(Supplementary Submission to No. 16)**
83	Telecom Australia now trading as Telstra Corporation Ltd **(Supplementary Submission to No. 23)**
84	Confidential Submission
85	Department of Employment, Education and Training
86	Department of Social Security **(Supplementary Submission to Nos. 36 and 73)**
87	Attorney-General's Department **(Supplementary Submission to Nos. 35 and 76)**
88	Australian Taxation Office **(Supplementary Submission to No. 34)**
89	Public Service Commission **(Supplementary Submission to No. 39)**
90	Commonwealth Director of Public Prosecutions **(Supplementary Submission to No. 6)**
91	Australian Federal Police **(Supplementary Submission to No. 14)**
92	Australian Postal Corporation **(Supplementary Submission to Nos. 30 and 64)**
93	Public Service Commission **(Supplementary Submission to Nos. 39 and 89)**
94	Attorney-General's Department **(Supplementary Submission to Nos. 35, 76 and 87)**
95	Telecom Australia now trading as Telstra Corporation Ltd **(Supplementary Submission to Nos. 23 and 83)**

96	Public Interest Advocacy Centre **(Supplementary Submission to No. 79)**
97	Attorney-General's Department **(Supplementary Submission to Nos. 35, 76, 87, and 94)**
98	Australian Federal Police **(Supplementary Submission to Nos. 14 and 91)**
99	Telecom Australia now trading as Telstra Corporation Ltd **(Supplementary Submission to Nos. 23, 83 and 95)**
100	Australian Postal Corporation **(Supplementary Submission to Nos. 30, 64 and 92)**
101	Australian Electoral Commission **(Supplementary Submission to No. 37)**
102	Telecom Australia now trading as Telstra Corporation Ltd **(Supplementary Submission to Nos. 23, 83, 95 and 99)**
103	Telecom Australia now trading as Telstra Corporation Ltd **(Supplementary Submission to Nos. 23, 83, 95, 99 and 102)**
104	Mr Peter Hallam **(Supplementary Submission to No. 28)**
105	Privacy Commissioner **(Supplementary Submission to No. 42)**
106	Commonwealth Director of Public Prosecutions **(Supplementary Submission to Nos. 6 and 90)**
107	Australian Taxation Office **(Supplementary Submission to Nos. 34 and 88)**
108	Comcare Australia
109	Department of Veterans' Affairs **(Supplementary Submission to No. 46)**

APPENDIX B

List of Exhibits

Exhibit Number		Exhibit
1	(i)	Hardy, M. 1992, 'Embassy in plea for guns', *Daily Telegraph Mirror,* 7 April, p. 1. Lagan, B & Norington, B. 1992, 'Witch-hunt after embassy blunder', *Sydney Morning Herald,* 8 April, p. 1 & 6. Norington, B. 1992, 'Seven to appear in court today', *Sydney Morning Herald,* 8 April, p. 6. Owens, W. 1992, "Rich' Iranians on dole', *Sunday Telegraph,* 12 April, p. 7.
	(ii)	Australian Taxation Office, 1990, *Safeguarding Your Privacy,* Brown & Co Typesetters Pty Ltd, Canberra
2		Australian Federal Police, undated, *Privacy Information Manual.*
3	(i)	Doherty, D & Middleton, Dr H. 1992, complaint document to Privacy Commissioner, on behalf of Anti-Bases Campaign, Sydney, 24 March.
	(ii)	Raper, M. 'Arms behind our backs', *Polemic,* **3**, Issue 1, 1992.
	(iii)	Privacy Commissioner, June 1992, Advice and Report to Ministers, Disclosure of Arrest Details of AIDEX Demonstrators: Australian Federal Police and Department of Social Security.
4		Australian Institute of Health and Welfare, undated, Information Security Policy and Procedures. AIHW Data Custodian Responsibilities. Undertaking for the Receipt of Constrained Information. Receipt of Constrained Information Schedule.
5	(i)	Health Insurance Commission, 1991, *Health Insurance Act 1973.*
	(ii)	Health Insurance Commission, 1991, *National Health Act 1953.*
	(iii)	Health Insurance Commission, undated, Guidelines for determining circumstances where the release of Confidential Information could be considered necessary in the public interest.
	(iv)	Ellicott, R. 1992, *Health Insurance Commission v Crymble & Another,* Opinion, March.

6 Cash Transaction Reports Agency, *Annual Report 1991-92.*

7 Confederation of Australian Industry (CAI), Business Council of Australia (BCA) and Australian Chamber of Commerce (ACC), 1985. 'Disclosure of Confidential Business Information', CAI, June.

8 (i) Australian Taxation Office, 1992, *Guide to Information Security,* AGPS, Victoria.

(ii) Australian Taxation Office, undated, *Code of Ethics,* AGPS, Canberra.

9 Australian Transaction Reports and Analysis Centre (AUSTRAC), *Extracts from Annual Report 1991-92.*

10 (i) Photocopies of newspaper articles, 1992, re: disclosure of information, (Main source, *The Age*).

(ii) Photocopies of newspaper clippings, 1992, which raise systems design (Main source, *The Age*).

11 (i) Public Service Commission, 1992, *Standard of Conduct,* National Capital Printing, Fyshwick ACT.

(ii) Public Service Commission, 1992, *Reprint of the Public Service Board's 1987 Guidelines on Official Conduct,* AGPS, Canberra.

(iii) Public Service Board, 1985, Personnel Management Manual, Vol. 3, *Personnel Practices,* AGPS, Canberra.

(iv) Public Service Commission, 1992, *A Framework for Human Resource Management in the Australian Public Service,* Microdata, Australia.

12 (i) Australian Federal Police, undated, *Security Classification Guidelines,* AFP 788.

(ii) Australian Federal Police, undated, *The Role and Function of Internal Security and Audit Division (ISAD).*

(iii) Australian Federal Police, 1991, *Personnel Security Within the AFP and Personal Privacy,* AFP785(12/91).

(iv) Australian Federal Police, 1992, *Police Records Checks Information Leaflet,* AFP 439C(7/92), and *Consent to Obtain Personal Information,* AFP 439A(7/92).

13 Department of Immigration, Local Government and Ethnic Affairs, 1992, 'Official Conduct of Staff', Administrative Circular, Canberra, AC 182,

14		Privacy Commissioner, 1992, Data-Matching in Commonwealth Administration, a Report to the Attorney-General.
15	(i)	Drugs of Dependence Unit (DDU), QLD, undated, Prohibitions and Authorities in Respect of Dangerous Drugs and Restricted Drugs, *Poisons Regulation 1973.*
	(ii)	Ministerial Council on Drug Strategy, 1992, *National Drug Strategic Plan 1992-1997.*
16	(i)	Confidential
	(ii)	Confidential
17		Privacy Commissioner, undated, extracts from *Personal Information Digest.*
18		Department of Finance, 1992, *Running Costs Arrangements Handbook, September 1992.*
19	(i)	Department of Administrative Services, undated, Guidelines for the Handling of 'Commercial-in-Confidence' Documents.
	(ii)	Department of Administrative Services, 1991, *Code for Handling Conflict of Interest,* AGPS, Canberra.
20	(i)	Department of Social Security, 1989, extracts from *Social Security Act 1991.*
	(ii)	Department of Social Security, undated, *Social Security Act 1991,* Determination under Section 1315 (Explanatory Statement).
	(iii)	Department of Social Security, undated, examples of Discipline Appeal Cases.
	(iv)	Department of Social Security, undated, Comparison of Penalties Imposed for Criminal Convictions.
	(v)	Department of Social Security, 1991, Procedure for Mail-Outs and Non-Standard Client Confirmation Exercises.
	(vi)	Department of Social Security, 1991, Departmental Correspondence to various businesses on the disclosure of confidential information.
	(vii)	Department of Social Security, 1992, Departmental Correspondence to various corporations on the disclosure of confidential information.

	(viii)	Department of Social Security's submission, 1991, to the Independent Commission Against Corruption (ICAC).
	(ix)	Department of Social Security, various dates, various departmental papers, instructions and guidelines on privacy.
21	(i)	Letter dated 6 May 1991, to Alan Cadman MP, from Senator the Hon Michael Tate.
	(ii)	Letter dated 15 November 1991, to Christopher Mann from the Commonwealth and Defence Force Ombudsman.
	(iii)	Letter dated 13 March 1992, to Christopher Mann from the Secretary, Department of Immigration, Local Government and Ethnic Affairs.
	(iv)	Affidavit dated 19 October 1992, of Vicki Seabrook, *Mann v New Medical Journals, Eccott and Fernyhough* (High Court of Justice (UK), Queens Bench Division).
	(v)	Affidavit dated 20 October 1992, of Martin David Alastair Bradshaw, *Mann v New Medical Journals, Eccott and Fernyhough* (High Court of Justice (UK), Queens Bench Division).
	(vi)	Sixth Affidavit of John Stanley Yerbury Rubinstein, undated, *Mann v New Medical Journals, Eccott and Fernyhough* (High Court of Justice (UK), Queens Bench Division).
	(vii)	Mann, C. undated, index and notes on understanding *The Rubinstein Report.*
	(viii)	John Stanley Yerbury Rubinstein, *Mann v New Medical Journals Limited, Ferynhough and Eccott,* report on visit to Australia – February and March 1987.
22	(i)	Letter dated 18 May 1990, to Privacy Commissioner from P G Bacich, NCPS Laboratories Pty Ltd.
	(ii)	Letter undated, to P G Bacich, NCPS Laboratories Pty Ltd from Privacy Commissioner.
	(iii)	Letter dated 25 June 1990, to Privacy Commissioner from P G Bacich, NCPS Laboratories Pty Ltd.
	(iv)	Letter dated August 1990, to P G Bacich, NCPS Laboratories Pty Ltd from Privacy Commissioner.
	(v)	Letter undated, to Privacy Commissioner from G Davidson, Australian Federal Police.

(vi) Letter dated 21 February 1991, to Mr J Lakos, Lakos & Company Solicitors, from M Mesaglio, Australian Federal Police.

(vii) Letter dated 4 March 1992, to Assistant Commissioner P W Baer, AFP, from P G Bacich.

(viii) Summons issued in the Supreme Court of NSW, dated 16 June 1992, in the matter of *Bacich v ABC.*

(ix) Judgement made by the Supreme Court of NSW, dated 1 September 1992, in the matter of *Bacich v ABC.*

(x) Letter dated 14 September 1992, to Assistant Commissioner P W Baer, AFP, from P G Bacich.

(xi) Letter dated 18 September 1992, to P G Bacich from Assistant Commissioner P W Baer, AFP.

23 Hughes, G. 'An Overview of Data Protection in Australia.' *Melbourne University Law Review* **18**, June 1991, pp. 83–120.

24 (i) Australian Postal Corporation, 'Change of Address' form PM15Q/Jul'93.

(ii) Australian Postal Corporation, Extract 'Divulging Information' from *General Procedures for Post Offices Manual.*

25 Northern Territory Police, 1991, for the National Police Working Party on Law Reform, submission to the Commonwealth Privacy Commissioner.

26 (i) Tucker, G. Prof. 'Frontiers of Information Privacy in Australia,' in the *Journal of Law and Information Science* **3**, 1992, No. 1.

(ii) Tucker, G. Prof. 'Present Situation and Trends in Privacy Protection OECD Area', *STI Review, No. 6, December 1989.*

(iii) Tucker, G. Prof. 1992, *Information Privacy Law in Australia.*

27 (i) Department of Social Security, 1993, *Confidentiality Manual.*

(ii) Department of Social Security, 1993, *The Right to Privacy,* DSS, Canberra.

(iii) Department of Social Security, 1993, *Privacy and the Department of Social Security - How we can help your clients and you,* DSS, Canberra.

(iv) Department of Social Security, 1993, *Everyone has a right to Privacy.*

	(v)	Department of Social Security, undated, National Instructions update, What is an Offence.
28	(i)	Privacy Commissioner, 1990, 'Data Matching in Commonwealth Administration', discussion paper and draft guidelines.
	(ii)	Privacy Commissioner, 1992, 'Data-matching in Commonwealth Administration – Guidelines and Commentary on Consultations', report to Attorney-General.
	(iii)	Australia, House of Representatives 1993, *Hansard,* 27 September, pp. 1152-3.
	(iv)	Attorney-General's Department, 1993, Critique of the Victorian Council for Civil Liberties Licensing Concept.
29	(i)	Telstra Corporation Limited, (Telecom Australia), 1993, copy of Administration contact letter.
	(ii)	Telstra Corporation Limited, (Telecom Australia), 1993, copy of Department Head letter.
	(iii)	Telstra Corporation Limited, (Telecom Australia), 1993, Interim guidelines for agencies approved to receive Telecom customer service information.
	(iv)	Telstra Corporation Limited, (Telecom Australia), undated, Data-matching information relating to Telecom and various agencies.
	(v)	Telstra Corporation Limited, (Telecom Australia), 1993, *Security in Telecom,* version 1.0, Telstra Corporation Limited 1993.
30	(i)	Confidential
	(ii)	Department of Social Security, undated, information on data-matching.
	(iii)	Department of Social Security, undated, data confidentiality – activities since 1992.
31		International Agency for Research on Cancer, 1994, Public Health, Epidemiology, Cancer Registries and Access to Name-Identified Data for Health Research.
32	(i)	Letter dated 29 May 1992, to Australian Federal Police from Privacy Commissioner.
	(ii)	Letter dated 27 July 1992, to Australian Federal Police from Australian Government Solicitor.

	(iii)	Letter dated 19 August 1992, from Dennis Rose QC, Chief General Counsel, to Australian Federal Police.
	(iv)	Letter dated 31 August 1992, to Australian Federal Police from Commonwealth and Defence Force Ombudsman.
	(v)	Letter dated 24 September 1992, to Australian Federal Police from Privacy Commissioner.
33	(i)	Telstra Corporation Limited, (Telecom Australia), undated, *Personal Information.*
	(ii)	Telstra Corporation Limited, (Telecom Australia), 1993, *Code of Conduct.*
34	(i)	Minute dated 14 August 1992, Telstra Corporation Limited, (Telecom Australia), concerning ICAC report into release of confidential information.
	(ii)	Telstra Corporation Limited, (Telecom Australia), Australian and Overseas Telecommunications Corporation's (ATOC) submission to the AUSTEL Inquiry into Privacy Implications of Telecommunications Services.
35		Department of Social Security, 1993, document relating to Disclosure of information to Commonwealth Departments and authorities revised arrangements - update.
36		Attorney-General's Department, 1993, Guidelines for the security of information systems.
37	(i)	Attorney-General's Department, 1992, copy of submission to the Secretaries' Committee on Intelligence and Security. Copy of letter dated 14 December 1992, to Senate Standing Committee on Legal and Constitutional Affairs from Attorney-General's Department.
	(ii)	Attorney-General's Department, 1991, review of the Protective Security Manual, Summary of PSM Implementation Survey.
	(iii)	Letter, dated 14 May 1992, and survey form, Survey Implementation of the Revised PSM.
38	(i)	Letter dated 24 September 1992, to Federal Member for Mitchell from the Commonwealth and Defence Force Ombudsman.
	(ii)	Department of Immigration, Local Government and Ethnic Affairs, internal minute dated 13 November 1991 to the Secretary.

(iii) Minute dated 2 October 1991, to Department of Immigration, Local Government and Ethnic Affairs', Legal Opinions Branch, requesting comments for the draft response to Mr Christopher Mann's complaint.

(iv) Letter dated 9 August 1991, to the Department of Immigration, Local Government and Ethnic Affairs from the Commonwealth and Defence Force Ombudsman.

39 (i) Confidential.

(ii) Letter dated 4 December 1992, to Privacy Commissioner from Australian Federal Police.

40 Statement from Mr R A Jessel, 1994, through Federal Member for Mitchell to House of Representatives Standing Committee on Legal and Constitutional Affairs, regarding Telecom Australia's Network Plus.

41 (i) Privacy Advisory Committee – Privacy Commissioner, 1994, *Outsourcing and Privacy,* Human Rights and Equal Opportunity Commission.

(ii) Privacy Commissioner, 1994, Report to the Attorney-General, 'Regulation of Data-Matching in Commonwealth Administration'.

(iii) Privacy Commissioner, 1994, *Plain English Guidelines to Information Privacy Principles 1-3.* Human Rights and Equal Opportunity Commission.

42 (i) Senate Estimates Committee B, 21 April 1992. Attachment A to Submission No. 107.

(ii) Australian Taxation Office, 1992, *Code of Ethics*, Cat. no. 92 2518 7, AGPS, Canberra.

(iii) Australian Taxation Office, 1994, *Guide to Information Security,* Cat. no. 92 1093 5, AGPS, Canberra.

(iv) Australian Taxation Office 1994, 'Draft Guidelines on Professional Conduct for staff of the Australian Taxation Office'.

43 Hon. George Gear, 8 December 1994, Contracting Out by Public Sector Agencies, *Industry Commission Act 1989.*

44 Provided by Ms Kathryn Favelle, Federal Bureau of Consumer Affairs, *Standing Committee of Officials of Consumer Affairs, Working Group on Direct Marketing, Discussion Paper, March 1995.*

45	Provided by Mr Peter Sekuless, submission, dated May 1995, by Australian Direct Marketing Association Ltd to Exhibit 44.
46	Provided by Ms Kathryn Favelle, Federal Bureau of Consumer Affairs, 'Ministerial Council on Consumer Affairs, Report of the Working Party on the Sale of Mailing Lists, July 1994'.
47	Provided by Ms Kathryn Favelle, Federal Bureau of Consumer Affairs, undated, 'Direct Marketing and the Australian Consumer, Discussion Paper'.
48	Provided by Ms Kathryn Favelle, Federal Bureau of Consumer Affairs, Second reading speech, dated 5 August, on New Zealand *Privacy of Information Bill.*
49	Provided by Ms Lynne Hunter, Information Officer, Delegation of the European Commission, dated 21 February 1995, Ref: IP/95/153, 'Council Adopts Common Position on Protection of Personal Data Directive'.

APPENDIX C

List of Witnesses

Sydney, Wednesday 30 September 1992

Private Citizen
Hon Adrian Roden QC

Melbourne, Tuesday 20 October 1992

Australian Transaction Reports and Analysis Centre
Mr William Coad, Director
Mr Neil Jensen, Director's Representative in Melbourne
Mr David Richardson, Special Projects Officer

Melbourne, Wednesday 21 October 1992

Australia Post
Mr Roger Cavanagh, Group Manager, Security and Investigation Service
Mr Christopher O'Meara, Senior Corporate Solicitor
Mr John Power, Group Manager, Letters
Mr Gerald Ryan, Secretary and Group Manager, Corporate Services

Australian and Overseas Telecommunications Corporation Ltd
Mr Christopher Devoy, Manager, Special Projects
Mr James Holmes, Corporate Secretary
Mr Michael Pickering, Manager, Information and Privacy, Regulatory Directorate

Law Reform Commission of Victoria
Mrs Loane Skene, Principal Research Officer

Victorian Council for Civil Liberties
Dr June Factor, Committee Member
Mr John Lanigan, Member

Monash University
Ms Susan McKemmish, Senior Lecturer, Graduate Department of Librarianship, Archives and Records
Mr Franklyn Upward, Lecturer, Graduate Department of Librarianship, Archives and Records

Canberra, Tuesday 27 October 1992

Attorney-Generals' Department
Mr Peter Ford, Assistant Secretary, National Security Branch
Mr Steven Marshall, Senior Government Lawyer, National Security Branch
Mr Norman Reaburn, Deputy Secretary
Ms Joan Sheedy, Senior Government Counsel, Human Rights Branch

Public Service Commission
Mr Edmund Attridge, Acting Deputy Commissioner
Mr Ian Edwards, Director, Ethics and Conduct
Mr Brian Gleeson, Acting First Assistant Commissioner, Management Selection and Development Division
Mr Richard Harding, Assistant Commissioner, People Management and Deployment Branch

Department of Social Security
Mr Sepp Babler, Assistant Secretary, Security and Control
Ms Patricia Faget, Director, Privacy
Mr Allan Ross, Assistant Secretary, Privacy and Review
Mr Michael Sassella, Principal Adviser, Legal Services Group
Mr Derek Volker, Secretary

Australian Customs Service
Mr James Fox, Assistant Director, Coordination, Executive Support
Mr John Hawksworth, National Manager, Investigation

Health Insurance Commission
Mr John Bentley, Assistant General Manager, Personnel
Mr John Brewer, Secretary
Mr Christopher Farrelley, Manager, Systems Operations Branch
Mr Kenneth Hazell, Assistant General Manager, Health Benefits Division

Canberra, Wednesday 28 October 1992

Australian Taxation Office
Dr Anthony Butterfield, Assistant Commissioner, National Office and Services
Ms Margaret Haly, Assistant Deputy Commissioner
Mr Amarjit Verick, Assistant Commissioner, Appeals and Review Group
Mr John Wharton, Director, Privacy

Australian Federal Police
Mr Ivar Lenfield, Serjeant, Legal Branch
Mr Daryl Smeaton, Assistant Secretary, Government and Public Relations
Mr Adrien Whiddett, Deputy Commissioner Administration

Office of the Federal Director of Public Prosecutions
Mr Ian Bermingham, First Assistant Director
Mr Geoffrey Gray, Assistant Director
Mr Edwin Lorkin, Associate Director

Department of Immigration, Local Government and Ethnic Affairs
Mr Emil Joseph, Assistant Secretary, Entry Branch
Mr Ian McIntosh, Assistant Secretary, Systems Branch
Mr Bob Malone, Assistant Director, Entry Systems and International Movement Records Subsection
Mrs Leila Stiernborg, Public Affairs Officer
Mr Mark Sullivan, First Assistant Secretary, Entry, Compliance and Systems Division
Mr Douglas Walker, Director, Legal Policy Section

Australian Electoral Commission
Dr Robin Bell, Deputy Electoral Commissioner
Mr Phillip Green, Director, Research, Legislative Projects and FOI

Melbourne, Tuesday 21 September 1993

Victorian Council for Civil Liberties
Dr June Factor, Committee Member
Mr John Lanigan, Assistant Secretary

Hunt and Hunt Solicitors
Dr Gordon Hughes

Telstra Corporation Ltd (Telecom Australia)
Mr David Harris, Manager, Personnel and Physical Security
Mr James Holmes, Corporate Secretary
Mr Michael Pickering, Manager, Corporate Policy

Private Citizen
Professor Gregory Tucker

Australia Post
Mr Christopher O'Meara, Senior Corporate Solicitor
Mr John Power, Manager, Letters Group
Mr Gerald Ryan, Secretary

Canberra, Wednesday 3 November 1993

Human Rights and Equal Opportunity Commission
Ms Christine Cowper, Senior Policy Officer
Mr Kevin O'Connor, Privacy Commissioner
Mr Michael Londey, Policy Officer

Attorney-General's Department
Mr Andrew England, Acting Principal Counsel, Human Rights Branch
Mr Peter Ford, Assistant Secretary, National Security Branch
Mr Steven Marshall, Senior Government Lawyer, National Security Branch
Ms Joan Sheedy, Senior Government Counsel, Human Rights Branch

Canberra, Thursday 10 February 1994

Australian National Audit Office
Mr Warren Cochrane, Acting National Business Director
Mrs Merran Dawson, IT Audit Consultant
Mr John Meert, Group Director, Performance Audit Business Unit
Mr Allan Millican, Senior Director (DSS Portfolio), Efficiency Audit
Ms Lorraine Partridge, Senior Auditor

Department of Social Security
Mr Sepp Babler, Assistant Secretary, Security and Control
Mr Anthony Blunn, Portfolio Secretary
Mr Robert Davidson, Director, Development Audit
Mr James Humphreys, National Manager, Operations
Mr Allan Ross, Assistant Secretary, Privacy and Review

Australian Institute of Health and Welfare
Dr Bruce Armstrong, Director
Mr Paul Jelfs, Research Fellow, Health Monitoring Division

APPENDIX D

Privacy Act 1988, Section 14 Information Privacy Principles

Information Privacy Principles

14. The Information Privacy Principles are as follows:

INFORMATION PRIVACY PRINCIPLES

Principle 1
Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

(a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

(b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2
Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

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

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3
Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4
Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5
Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the record-keeper has possession or control of any records that contain personal information; and

(b) if the record-keeper has possession or control of a record that contains such information:

(i) the nature of that information;

(ii) the main purposes for which that information is used; and

(iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

(a) the nature of the records of personal information kept by or on behalf of the record-keeper;

(b) the purpose for which each type of record is kept;

(c) the classes of individuals about whom records are kept;

(d) the period for which each type of record is kept;

(e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

(f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6
Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7
Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

(a) is accurate; and

(b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

(a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8
Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9
Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10
Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

(a) the individual concerned has consented to use of the information for that other purpose;

(b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

(c) use of the information for that other purpose is required or authorised by or under law;

(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11
Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

(d) the disclosure is required or authorised by or under law; or

(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

APPENDIX E

Case studies of agencies referred to by the New South Wales ICAC

The Independent Commission Against Corruption conducted an investigation into the unauthorised release of information from numerous Government departments and agencies.[1] Although the investigation was necessarily concerned with the unauthorised release of New South Wales Government information, and the participation of New South Wales public officials, a significant amount of evidence was taken on the unauthorised disclosure of information held by the Commonwealth Government.

The Committee took up the issues raised by the ICAC report with witnesses to this inquiry. Some of the issues are discussed in the body of this report. The Committee decided to locate some of the detail relevant to these issues in this appendix.

1. Case study – Telecom Australia

1.1 The New South Wales ICAC made formal findings in relation to five identified Telecom employees. Of those employees, three were found to have sold confidential information about Telecom customers to private investigators, with an admission from each of those employees to having done so. The Telecom information sold by employees included silent telephone numbers and addresses. Given that the ICAC terms of reference did not include the sale or exchange of Commonwealth information, the Commission was unable to make findings of corrupt conduct in relation to these employees.[2]

1.2 Two other employees admitted selling New South Wales government information to private investigators, one employee having obtained that information in exchange for confidential Telecom information. As the actions of these two Telecom employees involved State government information, the ICAC found that both had engaged in corrupt conduct.[3]

1.3 Further evidence of disclosure of Telecom information by employees was given by a number of witnesses, however most of these employees were not identified by the relevant witness, and in one instance Telecom employees were named by the witness but were not identified in the ICAC report.[4]

1.4 The ICAC inquiry also heard evidence from Telecom employees that Telecom Australia itself had bought confidential information from private investigators, including the criminal histories of individuals. The ICAC concluded that Telecom Australia had bought confidential government information from private investigators and made a formal

---

1 ICAC, *Report on Unauthorised Release of Government Information*, August 1992, Sydney.

2 ICAC, op cit, pp. 341, 823 and 1144.

3 ICAC, ibid., pp. 437 and 911.

4 ICAC, ibid., p. 354.

finding that the authority had engaged in conduct liable to allow, encourage or cause the offence of corrupt conduct.[5]

2. Telecom's response

2.1 Three employees who admitted selling Telecom information resigned before Telecom disciplinary procedures could take place. Telecom sought advice from the Commonwealth Director of Public Prosecutions (DPP) as to whether criminal proceedings should be instituted however, it was decided there was insufficient evidence to prosecute these individuals.

2.2 Another employee had admitted to the ICAC that he had sold confidential information obtained from the New South Wales Roads and Traffic Authority (RTA), but rejected the evidence of a witness that he had released Telecom information to a private investigator. The ICAC found that this employee had engaged in corrupt conduct, however Telecom decided there was an insufficient basis for disciplinary proceedings and he remained with Telecom.

2.3 Court proceedings are under way against one of the five employees who were named in the ICAC report and admitted releasing confidential Telecom or State Government information.

2.4 Private investigators gave evidence to the ICAC of obtaining confidential Telecom information from other Telecom employees, however these employees were not identified in the ICAC report.[6] The Committee sought advice from Telecom as to whether the assistance of the ICAC had been sought to identify the employees referred to, and what subsequent action had been taken with regard to each employee.

2.5 Several named persons were not working for Telecom when named in the ICAC evidence, and identification of several others was doubtful.[7] Telecom accepted one employee's sworn denial of allegations by a private investigator. No action was taken against one other employee because it was standard practice to obtain government information from private investigators and was done with the authorisation of Telecom itself.[8]

3. Organisational changes within Telecom

3.1 The Committee sought advice from Telecom as to what structural changes had taken place within the organisation in response to the ICAC findings. The Committee was particularly interested as to whether Telecom had investigated to what extent the employee activities revealed in New South Wales are occurring in other States.[9]

---

5 ICAC, ibid., pp. 1169–1172 and 1176.

6 ICAC, ibid., see for example, p. 394, 499, 510 and 730.

7 Telecom, *Submissions*, pp. S1058–S1060.

8 Telecom, *Submissions*, pp. S1061–S1062.

9 Telecom, *Transcript*, p. 417.

3.2 In response to the ICAC finding that Telecom itself had obtained confidential information from private investigators, the organisation has since reviewed its procedures for the use of private investigators. Telecom believes that as a result of a number of organisational changes the environment which enabled the unlawful activities revealed by the ICAC to take place no longer exists.

3.3 Formerly, confidential client information was provided to law enforcement agencies for approved purposes under authorised arrangements through regional offices of Telecom's Protective Services Unit. It was through the New South Wales Regional Office of the Telecom Protective Services Unit that confidential information held by Telecom had been unlawfully released to private investigators and others.[10]

3.4 Post-ICAC, the Protective Services Unit has been disbanded in all States, and the function of providing confidential customer information to law enforcement agencies for approved purposes has been relocated to a centralised group within the Corporate Secretariat. Telecom considers that this arrangement will regularise the working contacts between Telecom employees and law enforcement agencies.[11]

3.5 A matter of particular concern to the Committee is the protection of silent number information and the need for Telecom to limit employee access to this information. Telecom has reviewed employee access to each of the organisation's data bases (including silent number information), for both those employees with proper authorisation and those who might be able to gain access without authorisation. On the basis of that review Telecom has developed a set of system standards which are to be mandatory for all new data systems, although not for existing data bases.

3.6 The Committee acknowledges the organisational changes made by Telecom to reduce unlawful releases of confidential information. The Committee recognises that the matter of secure data bases is also of commercial importance to Telecom with the entry of competitors in the telecommunications industry. Telecom has not however, satisfied the Committee that the unlawful activities of some New South Wales employees were not also occurring (or may still be occurring) in other States.

3.7 Nor has Telecom satisfied the Committee that an effective audit system is in place that would alert management to such unlawful activities. In light of the ICAC revelations concerning Telecom employees the Committee considers that such an internal mechanism is essential.

4. Case study – Australia Post

4.1 A number of ICAC witnesses gave evidence of having obtained confidential Australia Post customer information, most often the names and addresses of the holders of private post office boxes.[12] A number of Australia Post employees were named as the sources

---

10 Telecom, *Submission*, p. S1003.

11 Telecom, *Transcript*, p. 418.

12 ICAC, see for example pp. 374, 394, 435, 499 or 546.

of this information.

4.2 The ICAC wrote to those Australia Post employees who could be located, offering them the opportunity to respond to the allegations. No response was received from any of these individuals.[13] As the information that had been released was from the Commonwealth rather than the New South Wales Government, the ICAC made no finding regarding this matter and the Australia Post employees who had been named were not identified in the report.

4.3 Australia Post witnesses before this Committee were unaware that employees of Australia Post had been invited by the ICAC to give evidence and had chosen not to respond. Australia Post subsequently sought advice from the ICAC on this matter.

5. Australia Post's response

5.1 Australia Post advised the Committee that most of the Australia Post employees named by ICAC witnesses had in fact, resigned in 1988 at the time of an internal Australia Post investigation into confidential information handling practices in New South Wales.[14] A post-ICAC inquiry conducted by Australia Post concluded that the remaining employees named by ICAC witnesses had disclosed confidential information to other government agencies without proper authorisation, in the belief that they were acting in good faith and not for corrupt purposes. These employees have since been counselled.

5.2 Australia Post believes that these activities occurred as a result of a lack of clear communication to employees as to the proper procedures for handling requests for address information.[15] Yet despite this, Mr Gerald Ryan, Secretary of Australia Post, told the Committee of his strong belief that Australia Post had a ". . . very solid base of commitment to privacy".[16] Australia Post claims in particular, that it has a privacy focus both in complying with the Privacy Act, and in its advice to operational and managerial staff on privacy principles and their application.[17]

5.3 All Australia Post employees have been reminded of their legal obligations regarding the handling of confidential information. Additional training has been provided for staff in privacy issues and in the organisation's security and investigations service which, following the earlier review in 1988, took over responsibility for handling requests from government agencies for confidential information.

6. Comments

6.1 The Committee considers that there has been ample evidence that unauthorised disclosures were occurring within Australia Post, and considers it to be highly likely that

---

13 ICAC, pp. 374–375.

14 Australia Post, *Transcript*, p. 64.

15 Australia Post, *Transcript*, p. 464.

16 Mr G. Ryan, *Transcript*, p. 467.

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

such activities were occurring within Australia Post in other states. These activities indicate a failure by officers to understand their privacy obligations, and by senior managers to fulfil their obligations of guidance to staff. The Committee supports the approach by management of reminding employees of their obligations in handling confidential third party information and in providing additional training in privacy and security.

7. Case study – Australian Customs Service

7.1 The Australian Customs Service (ACS), by arrangement with the New South Wales Roads and Traffic Authority (RTA), has direct access to the latter's computer system. The ACS has no authority to release information from the RTA data base to any other department or agency.[18]

7.2 The ACS also holds a considerable amount of confidential information on behalf of other agencies including the Department of Immigration and Ethnic Affairs, the Australian Federal Police and the Australian Bureau of Statistics.[19]

7.3 Employees of the Intelligence Section of the ACS in New South Wales gave evidence to the ICAC of releasing RTA information to the employees of county councils and Australia Post. Some of this information was subsequently sold to private investigators. Confidential information was released in the belief that it was part of the employees' duties, and one witness admitted authorising employees under his supervision to release this information in the belief that it was an informal departmental practice. The ICAC received evidence that in return for the information the ACS officers provided, they received other information. There was no evidence the officers received payment for the released information, and the practice ceased when the ICAC inquiry commenced.[20]

8. Australian Customs Service's response

8.1 The response of the ACS to the ICAC findings was unique in that the ACS recognised the activities arose from a 'sort of mythology handed down within the intelligence area that this was standard practice'. Mr John Hawksworth told the Committee that the officers concerned thought their actions were in the interests of the ACS.[21] This, wrongly but widely held belief, he argued, was indicative of a systemic failure in the intelligence area of the ACS rather than aberrant behaviour by individuals. Most importantly, the ACS did not take the view that these activities were peculiar to New South Wales. Instead, it recognised the possibility that such activities could be occurring in ACS intelligence units in all regions and responded accordingly.[22]

---

18 ICAC, p. 375.

19 Australian Customs Service, *Transcript*, p. 243.

20 ICAC, pp. 375–378.

21 *Transcript*, p. 243.

22 Australian Customs Service, *Transcript*, p. 244.

8.2 Officers who had appeared before the ICAC were counselled, and advice was sought from the Australian Government Solicitor and the Director of Public Prosecutions as to whether additional action should be taken. No further action was considered necessary.

9. Case study – Department of Immigration and Ethnic Affairs

9.1 Six officers of the Department of Immigration and Ethnic Affairs were named in evidence to the ICAC as having released confidential passenger movement information without authority, to employees of New South Wales county councils. Those officers did not reply to the ICAC's invitation to respond to the allegations, and were not identified in the report.

9.2 An internal investigation found that information had been released in the belief that it was permitted under the *Privacy Act 1988*, and that the officers involved had received no money or benefit. The investigation concluded that disciplinary action was not appropriate. The officers were counselled and given training in their responsibilities under the Privacy Act.[23]

9.3 The ICAC had also heard evidence from employees of a major bank that it was standard practice for the bank to purchase international passenger movement information from a private investigator. So standard a practice was it that a printed request form, used by bank employees when seeking information from the private investigator, included provision for requesting immigration checks.[24] Despite this, the Department stated that it 'has a strong culture of protection of personal and commercial information, a culture that pre-dates the enactment of the *Privacy Act*.'[25]

10. Case study – Department of Social Security

10.1 Confidential information from the Department of Social Security was bought and sold by private investigators either directly from employees of that department, or obtained indirectly through an information exchange network.

10.2 One witness to ICAC, a retired employee of the Department of Social Security, testified that he had sold confidential information about departmental clients to a private investigator for 15 years. He continued this illegal activity after retirement, buying confidential information from a departmental officer for resale.[26] The ICAC was unable to make a finding that these unlawful activities constituted corrupt conduct as the sale of the confidential information did not involve either State Government information or employees.

10.3 Apart from the activities of individual employees in selling confidential client information, the ICAC found that it had also been a routine practice for a number of

---

23 Department of Immigration and Ethnic Affairs, *Submissions*, pp. S897–S898.

24 ICAC, op cit, pp. 472-478.

25 DILGEA, *Submissions*, p. S281.

26 ICAC, op cit, pp. 460, 1229

years for DSS employees to release information, on an unpaid basis, through the *information exchange network.*

11. Response by the Department of Social Security

11.1 The DSS stated that although the ICAC report alleged that there had been unauthorised and corrupt release of confidential information on a large scale over a long period of time, there was no evidence in the report to support that allegation. The DPP however, considered that there was a prima facie case in respect of two DSS officers. One officer admitted passing information to a state police officer to assist with police inquiries. Another retired officer admitted passing information to a private investigator for payment, and recruiting a third officer to supply information for payment.[27]

11.2 A total of 37 employees and ex-employees of the DSS were named by witnesses or gave evidence to the ICAC regarding the release of confidential information about the clients of that department. ICAC transcripts regarding 36 of these individuals were referred by the AFP to the DPP for decision as to whether prosecutions should proceed, however there was insufficient evidence in the majority of instances. Two employees of the DSS were prosecuted. DSS also took action under the *Public Service Act 1922* in these two cases.[28]

11.3 In addition to the findings of the ICAC, the Committee was advised by the DSS that there had been occasional instances where action had been taken under the *Social Security Act 1991* against employees who had wrongly released information.[29] Overall though, it was DSS's view that the extent of employees trading in client information was on a small scale, and that most of those officers named in the ICAC report had mistakenly released data to New South Wales Government employees through misunderstanding their authority under the Social Security Act.

11.4 Questioned as to the basis for this view, and as to what action had been taken post-ICAC to establish whether similar activities were occurring in other states and territories, DSS was unable to provide evidence of such review action having been undertaken.[30]

11.5 Clearly, the detailed nature of confidential information held by the DSS rendered it a particularly sought after commodity. The Committee heard evidence that the secrecy provisions and sanctions of the Social Security Act were not as effective as they needed to be to deter those individuals determined to engage in the trading of DSS information.[31]

11.6 An efficiency audit by the Australian National Audit Office into the Department further revealed the vulnerability of confidential client data to unauthorised disclosure.

---

27 DSS, *Submissions*, p. S453.

28 Department of Social Security, *Transcript*, p. 227.

29 ibid., *Transcript* p. 230.

30 ibid., *Transcript*, pp. 236–238.

31 Mr Adrian Roden QC, *Transcript*, pp. 4–5.

12. ANAO Report on the Department of Social Security

12.1 Following the release of the ICAC report on confidential information, the ANAO conducted an audit of the efficiency and effectiveness of the management and implementation of the protection of confidential client information from unauthorised disclosure within the DSS.

12.2 The ANAO audit found that the activities revealed by the ICAC were more than the occasional instance claimed by the Department, and that these unauthorised activities continued to occur after the ICAC report received widespread publicity.

12.3 To give some indication, in 1992–93 there were 17 proven breaches of the section 1312 confidentiality provisions of the Social Security Act, with 47 further cases being investigated.[32]

12.4 The ANAO audit also found that even with considerable management commitment to maintaining confidentiality of client information, other internal organisational arrangements can reduce the effectiveness of, or militate against, that objective.

12.5 The ANAO considers that a major risk factor within the DSS arises from the widespread access that the majority of DSS staff have to the client data base. Approximately 17,000 employees of the DSS in 300 offices have unrestricted access to confidential details of over 5 million people, including the capacity to print client's personal details and in some areas the capacity to download data to disc, which would facilitate the easy removal of confidential information from departmental premises. The ANAO considers that the DSS has not justified the extent of the widespread access of employees to client data.[33]

12.6 The ANAO concluded that other risk factors flowed directly from the inadequacies of the department's data confidentiality strategy itself. The components of the strategy lacked specific objectives and were not integrated, there was no clearly defined working arrangement between the two areas responsible for privacy and security, and staff were unaware of the function and responsibilities of the privacy unit within the DSS.

12.7 The practice of the DSS programming staff in using confidential client data to test systems functions and applications is evidence that training needs to be more effective in assisting staff to recognise and understand the privacy aspects of their day-to-day work. Further, this practice exposes confidential data to employees who do not have an operational need for that information.

12.8 The ANAO was particularly critical of the DSS's limited capability to monitor access to the data base, and recommended that the DSS consider the use of audit trails of accesses to the client data base. This matter was taken up by the Committee directly with the Department, which advised that it had now defined a cost-effective way of logging all accesses to the client database and which would be implemented shortly.[34]

---

32 Department of Social Security, *Transcript*, p. 530.

33 Australian National Audit Office, *Audit Report No. 23 1993-94*, p. 10–11.

34 Department of Social Security, *Transcript*, p. 545.