CHAPTER 1

THE ADEQUACY OF THE AUSTRALIAN LEGISLATIVE STRUCTURE

Introduction

1.1 The use of technology in pursuit of crime control has a long history. For example, English criminologist Edward Henry is credited with creating the first set of fingerprint records in 1901, exactly 100 years ago.[1] As will be discussed in detail below, through electronic, laser and information technology developments, fingerprint records are now available to all Australian police services for instantaneous cross-matching purposes. Such rapid access to information is, of course, a major bonus to effective policing where speed of response is critical.

1.2 While the range and sophistication of the forensic sciences has continued to develop over the past century, with DNA matching the most prominent contemporary example, recent growth of technology has been described as 'exponential and rapid'.[2] It is clear that initiatives in the forensic and related sciences, combined with developments in computer technology and in other technological areas, such as the invention of drug- and explosives-detecting ionscan machines, have come to play a prominent role in law enforcement's armoury and that their results have made a significant contribution in the pursuit of successful prosecutions.

1.3 Further, while many of the more sophisticated tools are not inexpensive, many others have become available at ever diminishing cost and provide quicker results, thus increasing their overall value to law enforcement. As operating environments become increasingly cost-conscious, especially in the public sector, greater reliance will be placed on technology rather than human resources for achieving ever-higher productivity at ever-lower costs. It is apparent that, while there will always be a role for traditional labour-intensive policing methods, they will be increasingly supplemented and complemented by technological aids.

1.4 The keys to the past successes of technology in law enforcement have been several, but two considerations in particular stand out for mention: the level of legislative recognition which has been given to their use and the extent of acceptance by the courts of evidence generated by technical means. Without statutory recognition, the collection of such evidence by law enforcement risks being declared inadmissible by the courts - with the result that the prosecution case may collapse. When backed with proper legislative support, such evidence is often sufficiently

---

1 See http://library.thinkquest.org

2 *Evidence*, p. 1.

irrefutable to encourage an early guilty plea, with the accompanying benefits to prosecution and court processes.

1.5 In this Chapter, the Committee will seek to assess the extent to which the Commonwealth, State and Territory governments have ensured that the legislative regimes within their respective jurisdictions which underpin the NCA's operations are keeping pace with emerging technologies. It should be borne in mind that the NCA's role is essentially to combat national complex organised crime. While it is a creature of Commonwealth statute, its status is recognised and its operations underpinned by complementary legislation in each State and Territory. It is the only law enforcement agency in Australia whose investigations are not limited by jurisdictional boundaries.

1.6 There is clearly an extensive and ever-growing range of technological aids available to the general community for crime avoidance and to law enforcement for crime control. The Australian Institute of Criminology's 1998 Trends and Issues paper entitled *Technology & Crime Control,* included as part of the AIC's submission to this inquiry, discusses many in impressive detail.[3] There is also no apparent shortage of devices available to the better-resourced criminals with which to seek to thwart the efforts of their pursuers. The submission of the Australian Bureau of Criminal Intelligence referred to the case of Brendan Abbott, the so-called 'Postcard Bandit':

> When apprehended, Abbott had access to not only firearms but also police radio frequency scanners, electronic lock picking devices, information on constructing electronic devices including listening devices, mobile phone SIM-cards, software and computer hardware to produce counterfeit identity documents, as well as a number of false documents including drivers licences.[4]

1.7 As noted in the Preface, in this report the Committee will only address the major technological issues with a *national* crime perspective - to also include *community* policing issues would be too extensive a topic for this inquiry and would also stray beyond the Committee's primary area of interest.

1.8 Several submitters noted that there are currently inadequacies and inconsistencies in the frameworks of the several Australian legislatures to cater for technological change and to enable law enforcement to combat emerging technological crimes. The Australian Federal Police (AFP), for example, noted that '[c]urrent legislation was enacted whilst these things [police access to information, people and places] were predominantly physical. Now, however, these things exist in cyberspace. Current legislation is not adequate because it is silent on law enforcement use of new technologies'.[5] It was also pointed out by the Australian Information

---

3 *Submissions,* pp. 2-6.

4 *Submissions*, p. 128.

5 *Submissions,* p. 61.

Industry Association (AIIA) that, despite the similarities in the nature of the offences committed, the major difference between off-line offences and their online equivalents is the absence of the physical element.[6]

1.9 Stress has also been placed on the inter-jurisdictional nature of technological crimes, especially those committed by organised crime groups. Computer-related crimes in particular represent a serious challenge to the current approach to law enforcement based on national and State/Territory boundaries. While one discussion point in this inquiry has been the continuing relevance of the current national system of law enforcement to this 'borderless' environment, the Committee believes that the key issue for its consideration in the context of this inquiry is the extent to which the Parliaments in whose jurisdictions the NCA is expected to operate are *unnecessarily* constraining its access to the use of new technologies in its fight against organised crime. The Committee is mindful that use of some of the emerging technologies for crime control carry downside risks, not least from human rights and privacy perspectives, and that these factors need to be carefully weighed before proposals are advanced which would expand the range of NCA tools and powers.

1.10 Modern policing needs to address crimes which will routinely cross domestic and international jurisdictions. While Chapters 2 and 3 deal with the national and international dimensions of electronic crime, in this Chapter the Committee looks at the new technology challenges for policing primarily within Australia, especially within the Federal system where the States and Territories have responsibility for addressing the vast majority of criminality.[7]

1.11 New technologies are enabling law enforcement to develop and deploy a range of forensic and technical support tools in support of its traditional functions of detection, investigation and prosecution. The most concise summary of the critical role of technology in modern law enforcement was given by Dr Grant Wardlaw, Director of the Australian Bureau of Criminal Intelligence, in the following terms:

> We obviously have everyday things like word processors and spreadsheets for use in analysis and prosecution, software programs being developed that map criminal activity and that give spatial and temporal behaviour patterns as well as indicating offender behaviour, improvements in surveillance technology, including listening devices and telephone interception, mobile phones and emails helping officers to continually keep in touch, and, of course, national systems such as CrimTrac and our own intelligence and information systems.[8]

---

6 *Submissions,* p. 70.

7 At *Submissions,* p. 190, the Attorney-General's portfolio submission stated 'The extent of crime impacting on Commonwealth interests, including serious offences, is increasing even though in numerical terms the majority of crime overall is a matter for State and Territory jurisdictions.' This is a reference to the fact that, in Australia, the most voluminous incidents of criminality such as burglary, assault, traffic offences, and the like are matters for State/Territory regulation.

8 *Evidence*, p. 94.

The emphasis of this Chapter is on the extent to which the NCA is assisted in ensuring that those who commit major, serious criminal acts are able to be brought to justice by its being given access to such new technologies.[9]

Australia's legislative structure

1.12 While police access to several of the technologies mentioned by Dr Wardlaw is restricted only by resource considerations, others are subject to Commonwealth, State and Territory legislation of the nature sought to be examined by the Committee's term of reference (a). In order to provide a conceptual overview of the operations of this legislative structure, the Committee reproduces from the New South Wales Law Reform Commission's May 1997 Issues Paper entitled *Surveillance* a description of the division of responsibility, current as at 1996, of the Commonwealth and the State of New South Wales:

- The use of aural surveillance devices connected to the telephone system is governed by Commonwealth legislation: *Telecommunications (Interception) Act 1979* (Cth).

- The use of aural surveillance devices by Commonwealth agencies in the investigation of Commonwealth drug importation offences is regulated by Commonwealth law: *Customs Act 1900* (Cth) s 219A-219K.

- The use of aural surveillance devices by the Australian Federal Police in the investigation of certain non-narcotics Commonwealth offences is regulated by Commonwealth law: *Australian Federal Police Act 1979* (Cth) s 12B-12L.

- Aural surveillance devices used in New South Wales by State agencies and not connected to the telephone system are regulated by New South Wales law: *Listening Devices Act 1984.*

- Aural surveillance devices used in New South Wales by Commonwealth agencies (not including the Australian Federal Police) [Committee note: including the NCA] for offences which are not Commonwealth narcotic offences are regulated by New South Wales law: *Listening Devices Act 1984.*

- There is no regulation of visual surveillance, photography or the use of video cameras.[10]

1.13 This framework essentially holds true for each State and Territory in which the National Crime Authority operates, although there are sometimes distinct

---

9 While the Committee must, by virtue of its statutory basis, concentrate on the NCA, its comments will clearly have broad resonance across law enforcement in general.

10 Reproduced from New South Wales Law Reform Commission, *Surveillance,* Issues Paper 12, May 1997, pp. 24-25. The report cited its source as: B Schurr *Criminal Procedure (NSW)* (Loose-leaf Service, LBC Information Services, 1996) at para 8.70.

differences in the approaches of the States in dealing with those matters that fall within their jurisdictional capabilities. Subsequent to this 1996-based analysis New South Wales has, for example, enacted legislation to extend the *Listening Devices Act* to the operation of listening devices capable of tracking and video monitoring.

1.14 These crime fighting technologies will be addressed below under three main categories as follows:

- telecommunications interception;
- visual and other forms of electronic surveillance; and
- information and intelligence systems.

1.15 The discussion then briefly addresses the relationship of the laws of evidence in relation to new technology. It concludes with an examination of the accountability processes involved in access to relevant technologies by law enforcement, especially in view of the invasion of privacy involved.

Telecommunications interception

1.16 Telecommunications interception (TI) is a form of electronic surveillance in that, in broad terms, it provides a capacity to monitor people's affairs by electronic means. In this report the Committee will deal with issues arising from TI separately from the other forms of electronic surveillance (which are addressed in the next section below) because the Commonwealth is constitutionally responsible for its regulation under its head of power over '[p]ostal, telegraphic, telephonic and other like services'.[11] It exercises its powers through the *Telecommunications (Interception) Act 1979* [the TI Act].

1.17 While most State and Territory law enforcement agencies have access to TI information, both through the TI Act and their own State/Territory 'mirror' statutes, the other forms of electronic surveillance - such as the use of listening devices - are constitutionally issues for State/Territory regulation. The Commonwealth has, however, seen fit to pass specific legislation for use of these other forms of electronic surveillance by Commonwealth agencies.

1.18 Unquestionably, evidence gained by means of telecommunications interception is a vital contributing factor in successful prosecution of serious criminal offences. The 1994 report into the long term cost effectiveness of telecommunications interception by Mr Pat Barrett (at that time a Deputy Secretary of the then Department of Finance) found that:

---

11 *Constitution* (Cth) s. 51(v).

> Telecommunications interception is a very effective part of an integrated framework of surveillance, it being both cost effective and generally effective.[12]

1.19 Similarly, Victoria Police have reported:

> telecommunications interception is an extremely effective investigative tool, enabling investigators to identify persons involved in, and the infrastructure of organised criminal activities, particularly drug trafficking syndicates. In many cases, the weight of evidence obtained through telecommunication interceptions against a defendant leaves them with no option but to enter a guilty plea, representing significant savings in police resources and court time.[13]

This sentiment was reinforced in the submission of the Victorian Government to this inquiry in relation to electronic surveillance generally.[14]

1.20 The most recent annual report into the operations of the TI Act stated that:

> Evidence obtained from the use of telecommunications interception has resulted in many arrests, the seizure of large quantities of prohibited drugs and criminal assets. Agencies have also commented that the very existence of a telecommunications interception regime serves to frustrate criminal enterprises.[15]

1.21 The significance of TI to law enforcement is demonstrated by the decision of the Commonwealth Government in the May 1999 Budget to provide an additional $8.082 million over four years under the National Illicit Drug Strategy to augment the NCA's and AFP's operational capacity to collect and process evidence obtained through telephone interception. It is noteworthy that surveillance in general is a costly exercise. The NCA has estimated that to run a surveillance team (both electronic and physical) of seven staff for one shift a day costs in excess of $600,000 per annum.[16]

Background

1.22 Prior to the commencement of the *Telephonic Communications Act 1960* there was no statutory prohibition on telephone interception in Australia. The 1960 Act prohibited telephone interception except in very limited circumstances. These included for national security reasons and to enable the Postmaster-General's

---

12 Barrett P.J., *Review of the Long Term Cost Effectiveness of Telecommunications Interception,* Department of Finance, March 1994.

13 *Telecommunications (Interception Act) 1979: Report for the year ending 30 June 1999*, pp. 41-2.

14 *Submissions*, p. 138.

15 *Telecommunications (Interception Act) 1979: Report for the year ending 30 June 2000*, p. 17.

16 NCA submission to Senate Legal and Constitutional References Committee inquiry into the management arrangements and adequacy of funding of the AFP and the NCA, February 2001, p. 27.

Department to trace 'nuisance calls' and for technical purposes. Interception for general law enforcement purposes was not permitted.

1.23 The 1979 TI Act, as originally enacted, enabled interception warrants to be granted only for the investigation of narcotics offences under the *Customs Act 1901*. Since 1987 the offences in relation to which warrants are obtainable have been extended and the number of agencies authorised to apply for interception warrants has increased.[17]

1.24 The broad objective of the TI Act is to balance the need to protect the privacy of communications passing over telecommunications systems within Australia while facilitating appropriate access for national security purposes and by law enforcement. It is designed to protect the privacy of communications passing over a telecommunications system in Australia by:

- prohibiting the interception of communications passing over a telecommunications system in Australia without a warrant; and

- prohibiting the use of material obtained from a lawful or unlawful interception except in tightly defined circumstances set out in the Act.[18]

1.25 The Attorney-General's portfolio submission detailed the essential features of the scheme by which law enforcement agencies are allowed to intercept telecommunications under warrant in accordance with Part VI of the TI Act in the following terms:

- only the AFP, the NCA and certain formally 'declared' State agencies may apply for warrants;

- warrant applications must be supported by an affidavit setting out the information required by the Act to enable the Administrative Appeals Tribunal (AAT) member issuing the warrant to form a view on the matters about which he or she must be satisfied before exercising the discretion to issue a warrant;

- a warrant may be directed at a particular, identified telecommunications service or to any service which a person named on a warrant uses or is likely to use (named person warrants);

- the warrant issuer specifies the duration of the warrant and may impose conditions or restrictions and, in the case of named person warrants, specify particular services which may not be intercepted under the warrant; and

---

17 The 1987 amendments followed a recommendation of Mr Justice Stewart's *Report of the Royal Commission of Inquiry into Alleged Telephone Interceptions*. The Bill was subject to review by a Joint Select Committee on Telecommunications Interception, chaired by S P Martin MP, which reported in November 1986.

18 Attorney-General's portfolio, *Submissions,* p. 213.

- the AFP retains responsibility for overall supervision of all interceptions.[19]

1.26 Part VII of the TI Act makes it clear that telecommunications interception is an act of such significance that its permissible use is restricted in pursuit only of certain serious criminal offences and in certain disciplinary proceedings against AFP officers, State police officers and Commonwealth and State public servants or officers accused of impropriety. These are called class 1 and class 2 offences. Class 1 offences include murder, kidnapping, and narcotics offences. Class 2 offences include offences punishable by imprisonment for life or a period of at least seven years and offences where the offender's conduct involves serious personal injury, drug trafficking or serious fraud.

1.27 As noted at the first dot point in para 1.25, the AFP and the NCA are prescribed in the TI Act as eligible to apply for interception warrants. The Act also provides for 'eligible authorities' to access intercepted information obtained by other intercepting agencies which is relevant to their investigations. 'Eligible authorities' are the police services of each State and the Northern Territory (the Australian Capital Territory being automatically included by virtue of its Agreement with the AFP for the provision of policing services in the Territory), the NSW Crime Commission, the NSW Police Integrity Commission, the Inspector of the Police Integrity Commission, the NSW Independent Commission Against Corruption (ICAC), the Queensland Criminal Justice Commission, the Queensland Crime Commission and the Western Australian Anti-Corruption Commission. The former Royal Commission into the NSW Police Service had also been an 'eligible authority' until its winding up on 26 August 1997. The Police Integrity Commission has assumed many of the Royal Commission's functions.

1.28 Additionally, under section 34 of the Act, if a Ministerial declaration is in force for an 'eligible authority' of a State,[20] then that authority (declared as an 'agency' for the purposes of the Act) can apply for and obtain interception warrants in their own right. As at 30 June 2000 such 'agency' declarations were in force for the Victoria Police, NSW Crime Commission, the NSW Police Service, ICAC, South Australia Police, WA Police Service and the NSW Police Integrity Commission.[21]

1.29 The Queensland Minister for Police and Corrective Services, Hon Tom Barton MLA confirmed in his submission that:

> Queensland legislation does not provide for telephone interception. State investigators can therefore only use telephone interception powers when involved in joint operations with agencies with these powers.[22]

---

19 *Submissions*, p. 213.

20 For the purposes of the Act the expression State includes the Northern Territory (section 5).

21 *Telecommunications (Interception) Act 1979. Report for the year ending 30 June 2000,* p. 5.

22 *Submissions*, p. 91.

This is because section 35 of the TI Act imposes a requirement for there to be in place parallel requirements in State legislation in relation to safeguards and controls on agency access to interception warrants as a precondition to the making of a declaration by the Commonwealth Attorney-General. Thus, all law enforcement agencies which are approved to apply for the issue of interception warrants in their own right operate under equivalent supervisory and accountability provisions, including in relation to inspection and reporting.

1.30 The Attorney-General's portfolio indicates that the TI legislation is designed to be technology-neutral - it applies to any form of communication passing over a telecommunications system whether by voice, fax, images or data. Therefore, it already applies broadly to modern forms of communication which pass over a telecommunications system at some stage, such as the Short Messaging System (SMS), email and other types of Internet communications.[23]

1.31 The final piece of the regulatory picture in relation to TI is contained in the *Telecommunications Act 1997* (Cth). While the principal purpose of the legislation is to regulate the telecommunications industry, Parts 13, 14 and 15 ensure that the industry provides reasonable, necessary assistance for law enforcement purposes. Part 15, in particular, generally requires carriers and carriage service providers to provide, at their expense, an interception capability for each of the services they supply to the public. This facility ensures that a warrant issued under the TI Act can in fact be executed.

Discussion

1.32 The TI Act has been extensively amended since its original enactment, although this process of incremental amendment has been criticised for its tendency to be years behind the telecommunications systems used by criminals for communication.[24] The brief outline of the current state of the legislation given above demonstrates that the particular issue of concern to the former NCA Chairperson, Mr John Broome in 1998 (set out in page xvii of the Preface) in relation to one anachronistic feature of the TI Act, has now been addressed by the Parliament. The passage of the *Telecommunications (Interception) Legislation Amendment Act 2000* (the TI Amendment Act 2000) which in particular introduced the concept of 'named person warrants', has specifically overcome Mr Broome's concern that the legislation was locked into the era of the traditional landline telephone. In its submission to this inquiry, Victoria Police noted:

> The new amendments provide for one warrant to cover all services used by a nominated criminal. A single warrant thus provides access to the multiple SIM and Pre-Paid cards or multiple telecommunications services used by a

23 *Submissions,* p. 213.

24 Confidential submission.

> criminal. This has improved the efficiency with which investigations may be undertaken.[25]

1.33 Previously, the Act had required an agency wishing to intercept all the telecommunications services used by a particular suspect to obtain a separate warrant for each service. The NCA's submission noted that guidelines issued by the Attorney-General's Department had emphasised that a warrant against a person can only be used as a measure of last resort, however.[26] The named person warrant provisions of the TI Amendment Act 2000 will also be subject to review in 2003.

1.34 In his Second Reading Speech in relation to the 2000 Bill the Attorney-General, the Hon Daryl Williams MP, said:

> The amendments … proposed in the Bill will build on and develop the existing legislative scheme to ensure that it continues to support law enforcement and security agencies in the face of developments in technology and the deregulation and globalisation of the telecommunications industry. We must do this if we are to be effective in the fight against crime.[27]

1.35 Evidence to the PJC's inquiry indicates that while the current legislation is a significant advance, especially following the amendments made in 2000, there are suggestions for its further development in view of the increasingly transnational nature of major, contemporary criminality. These include:

- extending the range of offences and assisting foreign investigations;
- extending the purposes for which TI information may be used;
- the Commonwealth devolving some responsibility for TI to the States;
- better regulating the activities of Internet Service Providers; and
- ensuring the currency of the Act's provisions.

The Committee discusses each issue below.

Extending the range of offences and assisting foreign investigations

1.36 The general nature of offences included as class 1 and class 2 offences under the TI Act was detailed in para. 1.26. The NCA submitted that:

> with the expanding use of the Internet and the parallel increase in the scope for Internet effected frauds, there is a case for extending the range of

---

25 *Submissions,* p. 54.

26 *Submissions,* p. 154.

27 House of Representatives, *Hansard,* 16 Feb 00, p. 13491.

> offences for which warrants may be obtained to any fraud offence committed by electronic means ... Other offences that could be considered for inclusion are offences relating to child pornography and stalking.[28]

1.37 The NCA added by way of explanation that the Internet is not simply used to assist the perpetration of offences (which is analogous to the use of a telephone) but is the means by which the offences are committed.

1.38 In the context of a discussion over the lack of arrangements for TI foreign cooperation, representative of the Commonwealth Director of Public Prosecutions, Mr Geoffrey Gray, informed the Committee that the Action Group into Electronic Commerce (AGEC - see footnote 41 for details) had given consideration to having the range of offences widened. He told the Committee:

> The general concept is that if people commit offences electronically then you should be able to go into the electronic medium to investigate them, but the list of offences under the Telecommunications (Interception) Act does not allow you to do that at the moment.[29]

1.39 The TI Amendment Act 2000 introduced the notion of a foreign intelligence warrant, but limited its availability to ASIO only. Mr Gray stressed that 'the fundamental principle [is] that investigative tools which are available to support Australian investigations should be available to support foreign investigations'. He noted, however, that in the law enforcement context there was a 'chicken and egg' problem in relation to TI legislation supporting foreign investigations: it is not clear whether the way forward is to add offences to the TI Act while claiming to support foreign investigations, or whether warrants should be sought for foreign investigations and then look at the offences involved.

1.40 A representative of the Attorney-General's Department, Mr Peter Treyde, added that, because TI is seen as being a highly intrusive investigative technique, the TI Act is framed to impose protective mechanisms on privacy and controls on use of TI information by Australian law enforcement agencies. There remains a concern about how the privacy of Australians can be properly protected when information is passed to foreign law enforcement organisations.[30]

1.41 The Committee appreciates that the current range of offences is prescribed under the TI Act to demonstrate Parliament's recognition that the act of 'tapping' a telephone by law enforcement is a substantial invasion of privacy and should therefore be restricted only to investigations into the most serious of offences. It also acknowledges that there are privacy concerns about the extension of TI powers in support of foreign investigations. However, there is clearly substance to the argument that consideration should be given both to updating the TI Act to accommodate the

---

28 *Submissions*, p. 155.

29 *Evidence*, p. 40.

30 *Evidence*, p. 51.

more serious emerging technological offences and to enable Australia to cooperate with trustworthy overseas law enforcement bodies in pursuit of serious transnational crime.

Recommendation 1: That the Government give consideration to the range of offences prescribed under sections 5(1) and 5D of the *Telecommunications (Interception) Act 1979* in the context of contemporary technological developments.

Recommendation 2: That the Government make TI-related foreign intelligence warrants available to law enforcement agencies.

Extension of purposes for which TI information may be used

1.42 The submission of the NSW Director of Public Prosecutions, Mr Nicholas Cowdery QC, noted that in the May 1997 report of the Royal Commission into the NSW Police Service, Commissioner Justice James Wood had made a number of recommendations for reform of State legislation in relation to electronic surveillance in general (which will be discussed in greater detail in the section below entitled 'Visual and other forms of electronic surveillance') and specifically in relation to TI. Again speaking generally, Mr Cowdery noted that some of the Wood recommendations had since been addressed, while others had not. He wrote:

> For example, despite the recent amendments to extend the use of telephone intercept product in proceedings integrally related to criminal proceedings, such product cannot be admitted in evidence in confiscation proceedings under the Criminal Assets Recovery Act 1990 (NSW) [CARA] (although it can be admitted in proceedings under the Proceeds of Crime Act and its State equivalents, and in Customs Act civil based confiscation litigation). The Wood Report recommended the amendment of the TI Act to allow intercept evidence to be admitted in civil based confiscation proceedings, such as those conducted under CARA (para 7.91).[31]

1.43 Since the publication of Justice Wood's report, the TI Act has been amended on three occasions and amendments made in November 1997[32] were the subject of specific review by the Telecommunications Interception Policy Review, which was completed in May 1999.[33] In its report the Policy Review noted that the 1997 amendments had extended the purposes for which intercepted information could be used in evidence. The report noted comment it had received from the Australian Privacy Charter Council that the amendments had represented an undesirable erosion of the important principle that intercept 'product' should only be used for purposes consistent with the serious crime and national security grounds for which the warrants were granted in the first place.

---

31 *Submissions*, p. 94.

32 *Telecommunications (Interception) and Listening Device Amendment Act 1997.*

33 Attorney-General's Department, *Telecommunications Interception Policy Review,* May 1999.

1.44 The Policy Review did not, however, accede to this call. Rather, it accepted an argument from the NSW Police Integrity Commission that the Act should be amended to enable intercepted communications that had been admitted into evidence in an 'exempt proceeding' to thereafter be admitted in any other proceedings. This recommendation was implemented in the *Telecommunications (Interception) Legislation Amendment Act 2000.*

1.45 A similar argument to that of Mr Cowdery in relation to the exclusion of the *Criminal Assets Recovery Act 1990* (NSW) was made by the NSW Crime Commission but, apart from making mention of the issue, it was not taken further by the Policy Review. Accordingly, the Committee is in no position to conclude whether the TI Act needs further extension as submitted by Mr Cowdery but draws the matter to the Government's attention.

1.46 In the next subsection, the Committee examines calls for the States to be given the right to determine whether the range of offences for which TI is available might be broadened.

The Commonwealth giving devolved responsibility over TI to the States

1.47 Commissioner Wood had made it clear in his report of his concerns about the TI Act, describing it as 'extraordinarily complex and the occasion of real difficulty in application'.[34] The subsequent amendments appear to have met many of the specific concerns raised by the Commissioner in his report. One point of particular concern to him has clearly not been addressed, however. This relates to his call for the:

> devolution of Commonwealth responsibility to the States, at least in relation to the selection of agencies which might use a TI power, and the offences for which it should be available. This is in recognition of the inappropriateness of the Commonwealth being involved in the enforcement of laws at the State level.[35]

1.48 He described the Commonwealth's decision to give the Royal Commission the status only of an 'eligible authority' and not 'agency' status under section 34 of the TI Act (despite the request having been made by the NSW Government, as required by the Act) as 'distinctly unsatisfactory' and a rebuff. He wrote:

> It is difficult to fathom why, in an inquiry involving issues of such profound importance to the people of NSW as the later inquiries revealed [into, for example, paedophile activity] the State should have been denied its wish to confer the full powers it desired on the agency it selected to carry out the

34 Royal Commission into the NSW Police Service, *Final Report,* Volume II, as cited in *Submissions*, p. 96.

35 ibid., p. 99.

> investigation. Certainly the refusal constituted a major restriction upon the Commission's ability to conduct its investigations.[36]

1.49 No submitter to this inquiry pressed this issue directly with the Committee. It caught the Committee's attention because it represented virtually the only issue - if not the only issue - where the Commonwealth rather than the States was being asked to consider giving up some of its constitutional powers in the national interest of future law enforcement coordination and cooperation.

1.50 Given that the NSW Police, NSW Crime Commission, ICAC and the Commission's 'successor', the NSW Police Integrity Commission have 'agency' status, the problem cannot lie with the adequacy of the State's mirror legislation. Rather, it appears that the Royal Commission's rejection by the Attorney-General was based on criteria implicit in the Act for an agency to qualify - that it is a permanent body set up to investigate serious crime, that it is independent and that it is subject to strict accountability requirements.[37]

1.51 This is clearly a complex issue, which probably explains why no submitter chose to raise it with the Committee in the context of such a broadly based inquiry. With the benefit of hindsight of the Royal Commission's achievements, it would not be difficult to sympathise with Commissioner Wood's view that his inquiry deserved a declaration as an intercepting agency because of the significance of the revelations it went on to make. It would also seem to be a fully democratic outcome that, given that the NSW Government had supported the declaration, it alone should be held accountable for the decisions it makes, in the same way that the Government of Queensland is accountable for having chosen the opposite path of not introducing mirror legislation for its own agencies, as noted in para. 1.29.

1.52 The Committee is aware that the NSW Crime Commission also raised similar arguments with the Policy Review, including that it does not seem appropriate that the Commonwealth - which has little constitutional responsibility for the bulk of major crime - should be stipulating the types of crimes for which particular types of surveillance should be used. [38]

1.53 While a delegation to the States in relation to TI would seem to be contrary to the argument underpinning much of this report - that the future of law enforcement in this country in relation to addressing serious inter-jurisdictional crime should be built on more 'national' approaches - the Committee notes that States will still play a critical role in determining their own intra-state law enforcement priorities. Having regard to the long and chequered history of TI (only a portion of which has been able to be

---

36 ibid., p. 100. [Note: While not provided as part of a submission to this inquiry, Commissioner Wood was trenchant in his criticism of the Federal Government's approach to the NSW Government's request for his Commission's direct access to TI in Chapter 1 of Volume 1 of his Final Report, Part K, pages 17-18.]

37 *Telecommunications (Interception) Act 1979: Report for the year ending 30 June 2000*, p. 56.

38 ibid., p. 57.

considered in detail by the Committee), it would be understandable for there to be some sensitivity on the part of the Commonwealth in contemplating giving the States a capacity to broaden the range of offences for which they might use TI information. However, the need for future cooperation between the tiers of Government is an absolute necessity.

1.54 It is also noted that the Commonwealth will be sensitive to Australia's international obligations. For example, Australia has ratified the *International Covenant on Civil and Political Rights* and is a member of the Organisation for Economic Cooperation and Development, both of which place on the Government an expectation to seek to protect privacy from arbitrary interference. Given that surveillance laws such as the TI Act are contrary to principles of privacy, the Commonwealth would undoubtedly wish to ensure that, in order to avoid international condemnation, proper guidelines and safeguards are in place to avoid claims of 'arbitrariness'.

1.55 The Committee recognises that the representations of Commissioner Wood and the NSW Crime Commission are considered and are not made without considerable prior forethought. In the context of comprehensive future discussions about the need for a more cooperative approach to law enforcement, the Committee believes that this issue should be one part of the agenda.

Recommendation 3: That the Commonwealth consult with the Standing Committee of Attorneys-General whether regulation of the use of TI could be delegated to the States and Territories within a continuing context of broad-based mirror legislation.

Better regulating the activities of Internet Service Providers

1.56 The role of Internet Service Providers (ISPs) in their capacity as carriage service providers under the *Telecommunications Act 1997* and, therefore, their obligations under the TI Act, was a matter of considerable discussion by witnesses. As noted above, carriers and carriage service providers have certain obligations under the Telecommunications Act to provide reasonable, necessary assistance for law enforcement purposes. The significance of cooperation between the telecommunications industry and law enforcement is demonstrated by recent statistics from the Australian Communications Authority that some 998,548 disclosures of information (essentially telephone subscriber details) were made in 1999-2000 by carriers, carriage service providers or number database operators in accordance with the provisions of part 13 of the Telecommunications Act. In excess of half of these disclosures were made for the purpose of the enforcement of the criminal law, with some 98% of all disclosures made by the major three carriers of Telstra, Cable & Wireless Optus and Vodafone.[39] The Act also gives the Federal Privacy

39 Senate Environment, Communications, Information Technology and the Arts Legislation Committee, Supplementary Budget Estimates 2000-2001, 30 November 2000, Answer to Question on Notice No. 57.

Commissioner a monitoring role in relation to disclosures of personal information for law enforcement purposes.[40]

1.57 The Action Group into Electronic Commerce (AGEC),[41] which was formed in 1997 by the Heads of Commonwealth Operational Law Enforcement Agencies to research the impact of electronic commerce on law enforcement, identified that one of the key issues in improving law enforcement's response to changing information technology as being 'facilitating appropriate record keeping standards for Internet Service Providers'.[42]

1.58 Several members of AGEC addressed this issue in their individual submissions to this inquiry, while the then Western Australian Minister for Police also raised a range of similar and related concerns. AGEC itself also placed a submission before the Committee to clarify its views, because it felt that there had been some misunderstanding of its position expressed in the Committee's hearings.

1.59 The NCA's submission stated:

> LEAs currently require the co-operation of ISPs to intercept Internet traffic or obtain subscriber details… However, a number of LEA operations indicate that investigators cannot be consistently assured of an ISP's assistance and the low level of regulation (e.g. the absence of formal registration and licensing) raises the risk of compromising an investigation.[43]

The submission went on to note that organised crime figures could establish ISPs, with obviously potential adverse consequences for law enforcement, and that ISPs are not required to retain user information and records that could assist in criminal investigations. Of particular concern to the NCA is the absence of a requirement on ISPs for some form of identity check of their customers.

1.60 In oral evidence the NCA's Mr Irwin stressed that:

> what is important is that the ISPs keep their records for a sufficient period of time to enable law enforcement to gain access to them, just as it gains access to call charge records from the carriers under the Telecommunications Act to indicate who has been talking to whom at what time, so that similar

---

40 In his submission the Privacy Commissioner, Mr Malcolm Crompton, noted that these monitoring powers are in fact quite limited. See *Submissions,* p. 269.

41 The AGEC is chaired by the Director of the Australian Transaction Reports and Analysis Centre, Ms Elizabeth Montano. Its membership includes representatives of the Australian Competition and Consumer Commission, Australian Centre for Policing Research, Australian Federal Police, Attorney-General's Department, Australian Customs Service, Australian Securities and Investments Commission, Australian Taxation Office, Department of Immigration and Multicultural Affairs, Director of Public Prosecutions and the National Crime Authority.

42 *Submissions,* p. 147.

43 *Submissions*, p. 157.

> information is available in relation to those people who are using the Internet to communicate. [Some ISPs cooperate] but at the moment it is entirely voluntary and…while there may be cooperation for law enforcement from the larger Internet service providers the smaller ones do not necessarily cooperate to the same degree.[44]

In making this latter observation, Mr Irwin was endorsing comment contained in the submission of the Australian Bureau of Criminal Intelligence that while the larger ISPs generally keep adequate records, many smaller ones do not, and that consideration should be given to requiring all ISPs to maintain records.[45] He also noted that the keeping of customer records in relation to the Internet was an issue for international attention and that the Council of Europe had proposed appropriate requirements in its draft Convention on Cyber-Crime.

1.61 The submission of the Hon Kevin Prince, the then Western Australian Minister for Police, put forward the view that:

> serious consideration should be given in Australia to placing uniform requirements on ISPs to keep specific logs and other information, relating to the use of their systems, that may be required to identify those involved in criminal activities … Self-regulation and codes of conduct are, with regard to the electronic information industry, insufficient to guard against criminal activities.[46]

The Minister expressed concern that, if ISPs choose to be uncooperative with State police, for criminal or other motives, there may be little that State authorities can do legislatively within their own jurisdictions to seek to enforce that cooperation. This is because of the possibility of Commonwealth legislation being found to take precedence over any State legislation. Given these circumstances, Mr Prince called on the Commonwealth to provide more effective legislation.

1.62 The Australian Securities and Investments Commission (ASIC) also submitted its concerns about the need for better regulation of ISPs.[47] Its submission foreshadowed that the Financial Services Reform Bill - to modernise the regulation of the Australian financial services industry - would also give ASIC some additional enforcement powers to combat computer crime. At the time of preparation of the ASIC submission, it was thought that the Bill would contain provisions to permit ASIC to serve a written notice requiring a person providing services as an ISP to maintain log records created during a specified period of time. It also drew attention to several other proposals expected to be in the Bill, such as a provision to enable it to make mirror images of hard drives of computers during the execution of search warrants and a provision enabling it to serve on an ISP a written notice requiring it to

---

44 *Evidence*, p. 5.

45 *Submissions,* p. 130.

46 *Submissions*, p. 109.

47 *Submissions*, p. 49.

immediately cease providing services where information is placed on the Internet in contravention of the Corporations Law.[48]

1.63 ASIC also offered an additional suggestion for the better regulation of ISPs from a law enforcement, rather than its own corporate regulation, perspective. It suggested that, following the precedent of the *Proceeds of Crime Act 1987,* provision be made for law enforcement to be able to seek a Supreme Court order to require ISPs to monitor transactions through a customer's account.[49]

1.64 The Internet Industry Association (IIA), Electronic Frontiers Australia (EFA) and the Australian Privacy Charter Council responded to these submissions, as did the Federal Privacy Commissioner in relation to the record-keeping and retention requirements for personal information. Ms Mary-Jane Salier provided the IIA's response at a Committee hearing. Ms Salier stressed the IIA's involvement in several governmental committees to assist with the development of regulatory policy and its pioneering role in developing codes of practice for online content regulation in Australia. The IIA had also recently established a Law Enforcement Taskforce, chaired by IIA Director and OzEmail CEO, Mr Justin Milne, to assist its members and law enforcement to address the types of issues being raised with the Committee. The thrust of Ms Salier's evidence was that ISPs are working with law enforcement on the development of appropriate strategies while seeking to ensure that the privacy concerns of their customers are addressed and that no unfair burdens are placed on the industry.

1.65 Ms Salier expressed the industry's concerns about the impact for the industry of the submissions referred to above. In particular she stressed that, in relation to the keeping of records, a distinction had to be made between the notion of records used for billing purposes, which detail when customers log in and log out of their service, and of records of what customers do once online. She placed particular stress on the fact that, unlike call charge records which law enforcement accesses from the major telecommunications carriers, ISPs are not engaged in supplying a point-to-point communications service. They keep no record of 'what sites [customers] visit, what transactions they conduct, what news groups they frequent and what chat sessions they participate in'. They have no need to know this information and such conduct would have privacy and cost implications.[50] She summarised her argument in the following terms:

> I strongly believe that privacy considerations dictate that there should be no general storage of the content of communication and that there should be no general access to the content of communications without the appropriate

48 The *Financial Services Reform Bill 2001* was introduced into the House of Representatives on 5 April 2001. The issues foreshadowed in ASIC's submission were not included in the Bill.

49 *Submissions*, p. 49.

50 *Evidence*, p. 108.

> checks and balances such as those that are currently laid out under the Telecommunications (Interception) Act.[51]

1.66 Electronic Frontiers Australia and the Australian Privacy Charter Council raised similar concerns about requirements for ISPs to keep transaction log records, also from a privacy and human rights perspective. EFA expressed particular concern about a situation where a public authority could gain access to 'a vast wealth of communications data without a ministerial or judicial warrant'[52] while the Council wrote:

> It is one thing to allow law enforcement agencies access, under carefully controlled circumstances and subject to rigorous safeguards, to records already maintained for other purposes. It is quite another to require organisations to effectively spy on behalf of the state - to retain 'intelligence' purely on the basis that it may become useful for law enforcement. To introduce such a requirement would completely upset the balance between privacy and law enforcement in our community and would be a major step down the road towards a surveillance society.[53]

1.67 AGEC subsequently submitted a clear statement of the position taken by law enforcement in these respects. In summary, AGEC stressed that there was no question of seeking records regarding the content of communications, since this was already covered by the provisions of the TI Act. The records being sought are only those which are routinely created by ISPs for billing purposes, which are analogous to the Call Charge Records and Call Associated Data generated by the telephony carriers, and which are governed by the Telecommunications Act. AGEC conceded that there are privacy considerations, but that these are not new considerations and that appropriate provisions and safeguards are largely already in place. The only real point at issue is the length of time that ISPs should be required to retain them.[54]

1.68 The Privacy Commissioner subsequently wrote, in response to AGEC's submission, that there have been calls to subject Call Charge Records to the same access regime as the content of telephone calls:

> The argument is that it is possible to build up a quite detailed picture of a person from traffic data and that where traffic data is used in this way it should be subject to the protection of the [TI Act]. If record-keeping requirements for ISPs carry potential to collate information that is revealing or intrusive then it is likely that higher privacy safeguards will be appropriate.[55]

---

51 Evidence, p. 114.

52 *Submissions,* p. 247.

53 *Submissions,* p. 272.

54 *Submissions,* pp. 254-256.

55 *Submissions,* p. 270.

1.69 There is common ground that storage of records carries costs and, naturally, the larger the ISP and the longer the required period of storage, the greater the cost burden is likely to be. AGEC argued that the cost of storage of records is reasonable when kept in a compressed format on CD ROM or tape. In any case, any costs incurred by ISPs in relation to TI-related requests are paid by law enforcement on a cost-recovery basis.

1.70 AGEC stressed that Australian law enforcement agencies had not yet determined a view on the period for which records should be retained although it was noted that UK agencies had nominated periods of:

- 12 months in a form allowing real-time or live access; and
- a further six years by either the ISP or a Trusted Third Party

in conjunction with proposed ISP record-keeping amendments to the UK's *Regulation of Investigatory Powers Act 2000*.[56]

1.71 The Committee accepts that the same public interest considerations which relate to law enforcement access to records of the telephonic service providers should apply to ISPs. The crux of the issue is that criminals will seek to communicate by whichever form of technology they believe has the least chance of either being intercepted or relevant details being made available to law enforcement. While there may be technical reasons why some services are less capable of being intercepted than others (for example, there is the issue of the capacity of law enforcement to decrypt online communications), and there may be technical constraints to ISPs tracking a customer's multi-point online access, the Committee is concerned to ensure that the legislative regime is not also an avoidable impediment to efficient law enforcement.

1.72 The Committee notes that, while a persuasive case has been made out for better regulation of ISPs, it accepts that it is not well placed to determine the exact details of any such regulation. As the IIA pointed out, the Telecommunications Act is based on the notion of a co-regulatory approach, which seeks to promote the greatest practicable use of industry self-regulation.[57] The international deliberations, discussed in Chapter 3, will obviously also need to be considered in any move to introduce a regulatory regime in Australia. The Committee was also unable to get a full appreciation of the NCA's particular concerns about the absence of both a registration and licensing scheme for ISPs and a requirement on ISPs for some form of identity check of their customers. Both of these issues, as well as that of a possible role for ISPs in assisting law enforcement with decryption, which is a prominent feature of the UK debate, are in the Committee's view matters of some moment.

---

56 *Submissions,* p. 256.

57 *Evidence,* p. 110.

1.73 Accordingly, while the Committee is firmly of the view that ISPs should be better regulated, it urges the parties to continue discussions with a view to finding an acceptable balance between the needs of both law enforcement and the industry.

Recommendation 4: That the Government give particular consideration to the appropriate level of regulation of Internet Service Providers to ensure their cooperation with law enforcement.

Ensuring the currency of the Act's provisions

1.74 While the Attorney-General's portfolio submission made the claim that the TI Act is drafted to be technology-neutral (see para 1.30) and therefore of broad, and seemingly timeless, effect irrespective of mode of communication, it also noted that the transformation of the telecommunications industry arising from the 1997 deregulation has only just begun:

> Further significant developments in the telecommunications market can be expected in the next few years as computer and telecommunications technologies converge. The Government will continue to monitor the legislation closely to ensure it meets law enforcement needs.[58]

1.75 The Committee received additional evidence which emphasised the need for a system of continuous monitoring of technological developments to ensure that the TI legislation keeps pace. The specific issue of greatest concern was the emergence of strong encryption in telecommunications.

1.76 The NCA, for example, submitted that it had encountered a limited number of cases where criminals had used encryption to evade interception. It also noted that, following the Telecommunications Interception Policy Review, there had been established an Inter-Departmental Committee (IDC) on Cryptography, chaired by the Attorney-General's Department and comprising the Defence Signal Directorate, ASIO, AFP, Victoria Police, NSW Police Service, and the National Office for the Information Economy (NOIE).[59] The Committee notes the broad public sector representation on this inter-agency group and urges it to consult with private industry to ensure that its deliberations are realistic and capable of implementation in practice.

1.77 The Wood Royal Commission had included a call for the Government's consideration of 'an effective and workable regime for the continuous monitoring of advances in technology that can prevent their introduction until suitable capacity for intervention is established and that ensures timely and proper amendment of the *Telecommunications (Interception) Act 1979* to meet any such advance and current

58 *Submissions*, p. 214.

59 *Submissions,* p. 157.

needs'.[60] In giving oral evidence, NCA Member Mr Marshall Irwin saw merit in the Royal Commissioner's view:

> It may well be that law enforcement should be given the opportunity to consider those pieces of technology [such as encryption] before they are actually applied and that the people who are providing them are required, before doing so, to make their systems interceptible… by law enforcement agencies.[61]

1.78 The Committee notes that in the *Cybercrime Bill 2001*[62] the Government has proposed that:

> A magistrate would be able to order a person with knowledge of a computer system to provide such information or assistance as is necessary and reasonable to enable the officer to access, copy or print data. Such a power is contained in the draft Council of Europe Convention on Cybercrime and will assist officers in gaining access to encrypted information.[63]

1.79 The Committee believes that it is vital for law enforcement to maintain its capability to intercept and decipher all communications. It calls on the Government to monitor software and hardware developments which, when used in conjunction with telecommunications services, may defeat the purposes of the TI Act.

Recommendation 5: That the Government ensure that the integrity of the TI Act is not undermined by emerging technology.

1.80 Finally in this discussion of TI, the Committee notes that convergence of telecommunications and computing technologies may force the hands of governments in bringing in cooperative legislative solutions. The NCA submission noted one of the ironies of the current Federal system:

> A sent but unopened email needs a TI warrant for interception. Once the email has been downloaded and opened by the recipient it is their property and a search warrant is required. This also applies to Short Message Services (SMS) and voice messages stored in remote locations. These issues complicate the investigative process and may expose covert investigations.[64]

---

60 *Submissions,* p. 95.

61 *Evidence,* p. 19.

62 See Preface, Footnote 13 for details.

63 Hon Daryl Williams MP, Second Reading Speech, House of Representatives *Hansard*, 27.6.01, p. 28641.

64 *Submissions,* p. 156.

1.81 Executive Director of the Australian Information Industry Association, Mr Robert Durie, drew attention to the likely impact of 'wireless' technology:

> wireless is going to be huge, if it is not already, and that is going to lead to ubiquity of access, dispersal, et cetera. If we think that a lot of people are online now and there are a lot of transmissions now, we have not seen anything yet.[65]

1.82 With the General Packet Radio Service (GPRS) wireless data can be delivered to any device whether it be a mobile, Personal Digital Assistant (PDA) or laptop. The information is read and actioned 'live' without copies being made. The Committee simply notes that the 'complications' of the investigative process referred to by the NCA in its submission seem slight when compared to the challenges of the future.

Visual and other forms of aural electronic surveillance

1.83 While physical surveillance of the actions of persons suspected of being engaged in criminal activity will undoubtedly continue to be an important part of the traditional approach to policing, emerging technology over the recent past has permitted law enforcement to substantially expand its capacity to conduct surveillance and, in the process, to collect high quality and compelling evidence against the perpetrators of crime. The NCA submitted that it uses a range of technologies to detect and investigate complex national organised crime:

> For example, investigators utilise electronic surveillance provided by listening devices, miniature video cameras, tracking devices, data capturing devices and telecommunications interception. Investigators also use cyber-forensics to retrieve and analyse data from computers.[66]

1.84 Having examined the telecommunications interception issue above, the Committee will give consideration in this section to the legislative regime which applies to the use of all other electronic surveillance methodologies. It is a substantial and complex topic and is one which has been much studied at both Commonwealth and State level over many years. It could indeed have been the subject of an inquiry by the Committee in its own right. Accordingly, in the interests of succinctness, the Committee will concentrate on the major conceptual issues involved and especially from the National Crime Authority's perspective.

1.85 The types of electronic surveillance discussed below are contentious because they relate particularly to targeted individuals, where the issue of personal privacy is at its most confronting. Governments generally legislate to prohibit use of such surveillance devices, subject to certain exceptions. One of the main exceptions is, of course, in relation to law enforcement where it is argued that the public interest in the investigation and prosecution of criminal activity overrides privacy considerations.

---

65 *Evidence,* p. 84.

66 *Submissions,* p. 146.

1.86 In this context, it is noteworthy that one of the most pervasive surveillance developments in our community appears to have occurred without legislative action. Policing of public places - which has become known colloquially as 'overt' surveillance[67] - has been significantly assisted by the use of enhanced closed circuit television and video technology, with reduced street crime one benefit.[68] The ABCI informed the Committee that offences such as malicious wounding, vehicle theft, robbery and attempted murder have been detected and that numerous offenders have been arrested.[69] The same principle - that there is no general legal rule to prevent the use of a camera to film a person or private property if no trespass is involved - applies also to surveillance of places open to lawful access by the public or places lawfully viewed from a public place.

1.87 Simple video surveillance is now routinely used by shops, commercial premises and workplaces for security reasons[70] and have the added benefit of assisting the detection of criminal offences. There are also clear privacy implications. But, as Justice Wood's report noted: 'law abiding citizens have little to fear from surveillance' and 'those involved in serious crime have no legitimate claim to plan or engage in their criminal activities in privacy'.[71] ABCI commented that it is probable that the community will become increasingly reliant on sophisticated surveillance systems as they go about their daily business in the future.[72]

1.88 The NCA directed its submission to its concerns about the adequacy of Commonwealth legislation and to the 'patchwork' of State and Territory legislation. The Committee draws attention at this point to the overview of the Australian legislative situation given in para. 1.12. The Committee will address each in turn.

Commonwealth legislation

1.89 The *National Crime Authority Act 1984* (NCA Act) is silent on what access the Authority has to surveillance technologies. While the *Australian Federal Police Act 1979*, for example, specifically refers to access to the use of listening devices by AFP personnel in the investigation of a narrow range of offences, the NCA has no such powers clearly declared in its own legislation. Most of its policing powers are in fact those held by its secondees, be they from the AFP or State and Territory police services. Additionally, the AFP submission made the point that:

---

67 See, for example, New South Wales Law Reform Commission Issues Paper 12 entitled *Surveillance*, May 1997, p. 7.

68 The Wood Royal Commission report had noted that in *Bathurst City Council v Saban* (1985) 2 NSWLR 704 it was held that there is no legal prohibition against the use of a video camera in a public place, to film a suspect in a criminal investigation. See *Submissions,* p. 104.

69 *Submissions,* p. 131.

70 Some jurisdictions have specifically legislated to regulate this aspect. Mr Nicholas Cowdery, NSW Director of Public Prosecutions, noted the passage in NSW of the *Workplace Video Surveillance Act 1988.* See *Evidence,* p. 167.

71 See *Submissions,* p. 96.

72 *Submissions,* p. 131.

> Current legislation is not adequate because it is silent on law enforcement use of new technologies. As a result, existing (police) powers and their application in cyberspace are perceived as ambiguous or non-existent… Legislation, therefore, needs to support and ensure the purpose of law enforcement.[73]

1.90 The NCA's powers of federal applicability are declared in general Commonwealth statutes, including in the TI Act and the Customs Act, while its access to powers in State and Territory legislation is subject to provisions in subsection 55A(2) of the NCA Act - only recently inserted by the *National Crime Authority Amendment Act 2000* - which declare that a law of a State may confer on the Authority a duty, function or power that is 'of the same kind' as a duty, function or power conferred on the NCA by Commonwealth legislation.

1.91 The NCA's submission referred to this latter situation as 'unsatisfactory' and went on to state:

> This uncertain test ['same kind'] should be replaced with a provision that clearly permits the use by the NCA of the full range of investigative powers provided by State and Territory legislation which, it is assumed, was the legislative intention. The ideal position would be for those powers to be expressly given to the NCA and its staff members in their own right under the NCA Act.[74]

1.92 It is illustrative of the point that the NCA and AFP submissions seek to make by drawing a comparison between the NCA Act and the legislation underpinning the operations of the Australian Security Intelligence Organisation (ASIO), Australia's principal security intelligence agency. The two organisations have much in common: they both need to operate in a covert manner in the pursuit of their missions and they both need to make use of contemporary surveillance technologies. ASIO differs from the NCA, however, in that it operates within the authority of relevant Commonwealth statutes while the NCA has a dual Commonwealth and State/Territory basis for its power.

1.93 The Parliament made some significant amendments to the *Australian Security Intelligence Act 1979* in November 1999.[75] ASIO subsequently reported that:

> In essence, the changes amount to a modernisation of [ASIO's] current powers to meet the challenges posed by new technology, and to enable ASIO to utilise available technology in the execution of its functions.[76]

---

73 *Submissions,* p. 61.

74 *Submissions,* p. 154.

75 *Australian Security Intelligence Organisation Legislation Amendment Act 1999.*

76 ASIO, *Report to Parliament 1999-2000*, p. 27.

This is, of course, one of the principal interests of the Committee's current inquiry in relation to law enforcement.

1.94 The three main areas of amendment contained in the 1999 ASIO Act as outlined in the Attorney-General's Second Reading Speech were:

- Several provisions to improve ASIO's ability to access information stored in computers. Mr Williams stated that the amendments were necessary given that information relevant to security is frequently stored as computer data. This was not a totally new power. ASIO was already able to examine computer information relevant to security under search warrants and telecommunications interception warrants. The new computer access provisions would allow ASIO to obtain access through other means than were previously permitted.

- A provision permitting the issue of warrants to ASIO authorising the use of tracking devices. The use of tracking devices would permit more efficient use of resources and the amendments were necessary as several State governments were at the time legislating to regulate their use by police and other members of the community.

- Provision was made for ASIO to be authorised to enter property and enter or alter an object for the purpose of installing, using, and maintaining a tracking device. The new provisions were similar to the existing provisions for ASIO's use of listening devices.[77]

1.95 The computer access provisions permit ASIO to gain remote access to a computer from an external computer and, if necessary, to make amendments to data on a computer. The explanatory memorandum stated that this latter aspect included modifying access control and encryption systems. The purpose is essentially to extend ASIO's TI power to emails and, by giving ASIO the ability to access such information via a distant terminal, it is clearly less intrusive and safer for the investigating officer than having to rely on physical search and entry warrant powers. The NCA's submission stated:

> In light of these *ASIO Act* amendments, it may be appropriate for the search warrant provisions in other Commonwealth, State and Territory legislation to be reviewed to ensure that they enable effective searches of computers and other electronic equipment, of the nature provided by the *ASIO Act*. Such provisions, together with closer relations with the [Australian intelligence community], will assist [law enforcement agencies] in circumventing encryption used by criminal syndicates by obtaining direct access to original messages and documents.[78]

77 House of Representatives *Hansard,* 25 March 1999, pp. 4363-64.

78 *Submissions,* p. 156.

1.96 The inclusion of a power to install tracking devices followed a recommendation to that effect in the Walsh report.[79] That report had noted that the absence of this investigative tool was a privation not only for ASIO but also for both the NCA and the AFP.

1.97 The Committee wishes to highlight one other important difference between these ASIO amendments and the NCA situation. ASIO's use of surveillance devices and telecommunications intercepts is subject to audit by the Inspector-General of Intelligence and Security. The Commonwealth Ombudsman, Mr Ron McLeod, has pointed out in his submission that, while his office conducts a specific audit role over the NCA's and AFP's record-keeping in relation to telecommunications intercepts, no similar external accountability arrangements exist for law enforcement's use of listening devices. Mr McLeod's submission stated:

> The question is posed whether the installation and use of listening devices, and the use of video and tracking devices can be regarded as any less intrusive in terms of the invasion of a citizen's right to privacy than a telecommunications intercept. I would support steps to establish more embracive accountability arrangements that would encompass the range of intrusive powers used by law enforcement agencies.[80]

While noting the resource implications for the office of the Commonwealth Ombudsman, the Committee agrees wholeheartedly with the principle that, in the interests of a consistent approach, his office should be given jurisdiction over the use by the NCA (and other relevant law enforcement agencies) of any surveillance device and not simply telecommunications intercepts.

1.98 As will be discussed below, the NCA's access to surveillance devices is largely dependent on State and Territory legislative authority. The Committee accepts the NCA's view that this arrangement is unhelpful and that the situation is best resolved by the inclusion in the NCA Act itself of clear references to the NCA's ability to utilise modern electronic surveillance devices, in a similar manner to that of the ASIO Act. In terms of specific amendments, the NCA pointed to the *Victorian Surveillance Devices Act 1999* as a valuable model.[81]

1.99 Mention should be made of one current development. The NCA's submission had called for the introduction of listening device warrants in respect of the movement of articles in the course of illegal activities by persons unknown at the time of the warrant. Such 'person X' warrants had been considered legal until the decision of the Victorian Court of Appeal in *R v Nicholas.*[82] The Parliament is currently considering

---

79 Walsh, G., *Review of Policy Relating to Encryption Technologies*, 10 October 1996. An edited version of the Walsh Report was released to the Electronic Frontiers Australia (EFA) organisation following a freedom of information application in June 1997 and EFA published it on the Internet at www.efa.org.au.

80 *Submissions,* p. 117.

81 *Submissions,* p. 152.

82 *R v Nicholas* [2000] VSCA 49.

the *Measures to Combat Serious and Organised Crime Bill 2001,* which contains appropriate amendments to the Customs Act that would implement the NCA's recommendation.

State and Territory legislation

1.100 Notwithstanding the problems the NCA experiences from the uncertainty of the 'same kind' provision referred to above, its submission stressed that State and Territory electronic surveillance legislation is a 'patchwork' which impacts adversely on its capacity to coordinate investigations against complex national organised crime, especially when separate warrants need to be obtained in several jurisdictions in the course of the one operation. The 'patchwork' nature of the varying State and Territory legislative provisions in relation to electronic surveillance was described in the following terms:

> The legislation in Victoria, Western Australia and Queensland provides for the use of a wide range of surveillance devices. [Footnote in orginal: The Victorian *Surveillance Devices Act 1999* refers to data surveillance devices, listening devices, optical surveillance devices and tracking devices. The Western Australia *Surveillance Devices Act 1998* refers to listening devices, optical surveillance devices and tracking devices but not to data surveillance devices. The Queensland PPR Act (*Police Powers and Responsibilities Act 2000*) refers to listening devices, visual surveillance devices and tracking device or any combination of those devices.] The legislation in New South Wales provides for composite listening/video and listening/tracking devices. Legislation in other jurisdictions is confined to the use of listening devices.[83]

1.101 The patchwork status of legislation raises the issue of the application of cross-border operations where what might be authorised in one State may not be similarly permitted in another. The NCA submission noted:

> For example, a listening device may be installed in a vehicle travelling across state and territory jurisdictional boundaries. Successful surveillance requires different and separate warrants to be obtained for each jurisdiction. This is a particular problem for the NCA investigations that have a national and international focus.[84]

1.102 Victoria Police's Detective Inspector Stephen Berriman echoed the NCA's concerns when he described the practical implications for the Victoria Police in relation to tracking a drug courier from Victoria to New South Wales:

> At this stage, we would take out a warrant in Victoria under the Surveillance Devices Act for a tracking device… Once it hits the border, it goes into New South Wales. The New South Wales legislation is silent on the use of

83 *Submissions,* p. 153.

84 ibid.

> tracking devices at this time, so there is no prohibition … We can still track it.[85]

However, if New South Wales were to introduce tracking devices legislation, Victoria Police would commit a criminal offence if it did not obtain an appropriate NSW warrant.

1.103 Both the NSW Director of Public Prosecutions, Mr Nicholas Cowdery QC, and Detective Inspector Berriman noted that, if a surveillance device operating pursuant to a warrant within one State travels out of the State, there could subsequently be evidentiary problems when the matter comes to court.[86]

1.104 Detective Inspector Berriman also explained to the Committee that the impediment to installing tracking devices at the federal level is the issue of 'trespass re-entry'. He said:

> There is legislative support to actually place a device on a vehicle or on an object, and for the entry to premises to retrieve it - and it may not be the same premises. Once you have placed these devices, particularly in a mobile environment, you have to have contingency plans to retrieve [them] … That is not possible without legislative support.[87]

The NCA's submission clarified that, while Victorian legislation might authorise the trespass where necessary to install a tracking device and a data surveillance device, no State other than Victoria permits data surveillance and the different States have differing provisions in relation to tracking devices. It stressed the 'important need' for all jurisdictions to enact legislation to authorise the 'trespass'.[88]

1.105 In his submission, Commissioner of the Northern Territory Police, Mr Brian Bates, made this general comment:

> It is recognised that there are current inadequacies within the Commonwealth, State and Territory legislative frameworks to cater for technological changes … policing needs to respond to technology in a coordinated and consistent manner to address crimes that will routinely cross domestic and international jurisdictions.[89]

1.106 The Committee has been down this path before. In its December 1999 report *Street Legal: The Involvement of the National Crime Authority in Controlled Operations* the Committee recommended that the Commonwealth, States and Territories should seek to introduce uniform controlled operations legislation. While

---

85 *Evidence,* p. 129.

86 *Evidence,* pp. 167, 130.

87 *Evidence,* p. 129.

88 *Submissions,* p. 154.

89 *Submissions,* p. 45.

the Commonwealth Government indicated its agreement to this recommendation, it saw the quest for uniformity as a 'medium term' goal while it agreed to press ahead with pursuing the enhancement of Commonwealth provisions in the first instance.[90]

1.107 This approach, while understandable, still suggests a regime of disparate legislation across jurisdictions for the foreseeable future, with criminals (and lawyers) the main beneficiaries. The ideal situation from a national perspective is national legislation. Australia also has been down this path before. The introduction of *The Corporations Law* in 1989 was one of the more prominent examples of national cooperation to overcome a national regulatory problem, despite the subject matter being constitutionally a State matter. Another was the introduction in 1996 of a National Classification Code for the classification of publications, films and computer games, although States retained the enforcement role in that case. Even as far back as the 1930s the States cooperated with the Commonwealth on the issue of the regulation of intrastate aviation, which system of regulation was patently contradictory to the national and international nature of the industry.

1.108 The Committee recognises that the States and Territories may wish to take a different view about the merits of national legislation in relation to the use of surveillance devices and computer-attack capabilities within their jurisdictions. In the submission of the then Australian Capital Territory Attorney-General (and now Chief Minister), Mr Gary Humphries MLA, he noted two areas where the ACT has no legislation in relation to law enforcement access to computer-based information, noting 'these matters have yet to be considered by the wider legal community in the ACT'.[91] As stated earlier, Queensland has introduced comprehensive surveillance devices legislation but has still not decided to introduce telephone interception legislation, even after some 20 years of practical experience elsewhere. Yet in 1998-99 the Queensland Police made seven arrests on the basis of intercepted information obtained under warrant by either the NSW or Victoria Police.[92]

1.109 The NSW Director of Public Prosecutions, Mr Nicholas Cowdery, stressed his view that legislation in NSW had lagged behind developments in the technology available to law enforcement agencies. He drew attention to the recommendation of the NSW Drug Summit 1999 that the law relating to electronic surveillance, listening devices, search warrants and controlled operations should be urgently enhanced to assist police in quickly targeting drug traffickers.[93] Mr Cowdery also noted that the NSW Law Reform Commission had commenced an inquiry into the law relating to electronic surveillance in July 1996, had issued an Issues Paper in May 1997 entitled *Surveillance* and had finalised its interim report in February 2001. At the time of writing, this interim report had not been published. Finally, Mr Cowdery highlighted

---

90 Senate, *Hansard,* 29 March 2001, p. 23361. See Measures to Combat Serious and Organised Crime Bill 2001 for details of the Government's initiatives in this respect.

91 *Submissions,* p. 65.

92 *Telecommunications (Interception) Act 1979*: *Report for the year ending 30 June 1999,* p. 42.

93 NSW Drug Summit 1999, *Communique*, 21 May 1999, para 9.15.

the recommendations of the Wood Royal Commission on the need for the State's *Listening Devices Act 1984* to be updated. Some of the problems identified have been resolved in more recent amendments, while others remain.[94]

1.110 In general terms, the current patchwork of State and Territory legislation speaks for itself. This level of variation at the State and Territory level does not bode well for agreement on national legislation in the short term, although the Committee was heartened by the advice of Mr Karl Alderson, a senior officer of the Attorney-General's Department, that under the auspices of the relevant Ministerial councils there is a dedicated group of Commonwealth and State experts on uniformity and consistency of law enforcement legislation.[95] As the Government stated in reference to uniform controlled operations legislation, progress is more likely to be a medium term goal.

1.111 However, there is one possibility which could prompt this matter to gain momentum: the development of an international convention which, should Australia become a signatory, might provide the Commonwealth with constitutional authority under its 'external affairs' power to introduce national legislation which would override State and Territory legislation to the extent of any conflict or inconsistency. As detailed in Chapter 3, much work on cross-jurisdictional computer-based crime is being undertaken, such as that of the Council of Europe Draft Convention on Cyber-Crime. And, as pointed out by the Federal Privacy Commissioner, a small country like Australia may find itself having to be a policy taker in areas which may not always or in all respects fit well with our legal system or structure, given the adverse consequences which might flow from non-cooperation.[96]

1.112 The Committee notes that, with such awareness of the need for the standardisation of laws at the international level, it can only be a matter of time before Australia will have to commit itself to a similarly cooperative scheme at the national level.

1.113 In the absence of agreed national legislation the NCA, Victoria Police and Mr Cowdery suggested that the issue can best be dealt with by the making of uniform amendments to the respective State and Territory surveillance devices legislation to provide for extraterritorial operation and mutual recognition.[97] The use of technology neutral language, which will incorporate all existing and foreseeable devices, is also seen as desirable. Thus, under a fully national cooperative scheme, any warrant issued in one jurisdiction for anything of a surveillance devices nature would not only be declared as having effect across State borders at the time of its issue, but would also be granted validity within the law of the 'receiving' State. Recent amendments in

---

94 *Evidence,* p. 166, and *Submissions,* pp. 93-94.

95 *Evidence,* p. 45.

96 *Submissions,* p. 260.

97 *Submissions,* pp. 153-54, and *Evidence,* pp. 130, 166.

section 195 of the Queensland *Police Powers and Responsibilities Act 2000* are seen as providing a model in this respect. This process has been depicted as one of 'harmonisation' of the disparate State and Territory legislative regimes, which is an apt description given its current discordant state.

1.114 The NCA noted with approval the introduction in the United Kingdom of the *Regulation of Investigatory Powers Act 2000* as a model for Australia. That Act contains provisions that go beyond the types of investigatory powers currently accepted as the norm in legislation in Australia and its introduction in the UK has not been without considerable controversy. However, it is more the manner in which the Act codifies relevant laws for the whole country that the NCA has sought to endorse. In terms of certainty of the operations of the law, it would seem sensible to add (or, indeed, delete) investigatory powers within the framework of a single piece of legislation, rather than having them scattered throughout the statute books.

1.115 The UK Act is designed to ensure that the relevant investigatory powers are used in accordance with human rights. It encompasses the interception of communications, intrusive and covert surveillance, the use of covert human intelligence sources (such as agents, informants and undercover officers), the acquisition of communications data; and access to encrypted data. Importantly, for each of these powers, the law clearly states the purposes for which they may be used; which authorities can use the powers; who should authorise each use of the power; the use that can be made of the material gained; independent judicial oversight; and a means of redress for the individual.

1.116 In the Australian situation, emphasis would need to be placed on the types of provisions currently contained in the *Telecommunications (Interception) Act 1979* such as the need for judicial supervision of the investigatory processes, uniform oversight of the adequacy of all administrative processes by the relevant Ombudsman,[98] and high standards of accountability through reporting to the Minister and the Parliament.

Recommendation 6: That, in conjunction with the States, the Government introduce comprehensive national electronic surveillance legislation, with particular emphasis on the inclusion of appropriate privacy provisions.

Information and intelligence systems

1.117 While information technology (IT) is playing an ever-increasing role in criminal activity - with traditional crimes such as fraud and the exchange of child pornography now performed in an online as well as the offline environment - the efficiency of law enforcement has also been significantly assisted by IT developments. Agencies such as the NCA gain considerable benefit from the use of current technologies in the management and storage of information and intelligence systems. The NCA's submission detailed a case study of an investigation into large-scale tax

98 The Commonwealth Ombudsman currently oversights the use of TI by the NCA and the AFP.

evasion where large amounts of documentary evidence and IT evidence gathered from the hard drives of seized computers was able to be analysed by use of sophisticated computer applications.[99]

1.118 The benefits of such modern IT developments to any one law enforcement agency tend to be limited more by budgets than by the quality of legislative support to their use by governments, which is the Committee's principal interest. However, one of the more important aspects of IT in law enforcement is the manner and extent to which agencies are able (and willing) to exchange their valuable intelligence material with each other. While bilateral, agency-to-agency transfers of information would occur regularly under Memorandums of Understanding, the development of multilateral exchange has required the active involvement of the several Australian governments. This process has led in particular to the establishment of two agencies: the Australian Bureau of Criminal Intelligence (ABCI) and the CrimTrac Agency.

1.119 The ABCI was established in 1981 to improve intelligence cooperation and coordination between Australian police services. At that time it dealt with just eight police services - it now has in excess of 38 agencies with which it exchanges law enforcement information. It is non-operational and relies on client agencies for the collection of information in the field. Funding of the ABCI reflects its national character. Being established as one of the national common police services under the jurisdiction of the Australasian Police Ministers' Council, it is not a Commonwealth agency but it nonetheless receives the bulk of its funding from the Commonwealth Government, as well as supplementation from State government sources.

1.120 To achieve its goals it provides a range of IT services, training programs and analytical assistance to its client agencies. Access to ABCI information is through the Australian Law Enforcement Intelligence Net (ALEIN). ALEIN is a secure, national extranet used by all Australian police services and a large number of government law enforcement agencies. It is a universal system that fosters the sharing of criminal intelligence, especially as its use is not dependent on the type of hardware in use by the client agency. Through web browser technology, ALEIN acts as a gateway to the ABCI's document-based reference material and structured databases such as the Australian Criminal Intelligence Database (ACID) and the Violent Crime Linkage Analysis System.

1.121 The ABCI acts as a custodian of the information placed on its systems by law enforcement agencies. Importantly, given that management of criminal intelligence is an important issue for all law enforcement agencies, the client agencies retain ownership and control of their data.[100]

---

99 *Submissions,* p. 158.

100 *Submissions,* p. 136.

1.122 The NCA uses ACID and ALEIN as the repositories of intelligence for the task forces it coordinates under the NCA Act[101] but its submission to this inquiry emphasised that its capacity to disseminate information to some agencies was uncertain because of doubts about whether they are 'law enforcement agencies' for the purposes of the NCA Act. This is taken to be a reference to section 59 of the NCA Act. Regrettably, while the Government has proposed amendments in the *National Crime Authority Legislation Amendment Bill 2000 [2001]*, which was before the Parliament at the time of compilation of this report, to amend section 59 to enable the NCA's Chairperson to disseminate information to foreign law enforcement agencies, it failed to define with greater clarity to which domestic law enforcement agencies the NCA Chairperson can provide information. The Committee draws this matter to the Government's attention.

1.123 The ABCI noted, and the submission from Canberra-based software company, The Distillery Pty Ltd confirmed,[102] that information cooperation is far from perfect because law enforcement is subject to restrictions on the use to which it can be put. The ABCI submitted:

> Privacy, Freedom of Information, Call Charge Records (CCR), telephone interception (TI) information and the requirement to restrict data collected by use of coercive powers is placing such a legislative and resource burden on agencies that they are often unwilling or unable to put information into databases such as ACID. In cases where agencies do include intelligence which might be tainted with CCR or TI information, it is usually caveated to such a degree that it is unavailable to other law enforcement officers around Australia.[103]

1.124 The Committee recognises that some constraints on the use to which law enforcement information can be put are desirable, but it also notes that for databases to be effective, maximum cooperation is desirable.

Recommendation 7: That the Australian Government place on the agenda of the Standing Committee of Attorneys-General the need for a comprehensive and fundamental review of the operations of legislative provisions that may inadvertently and unnecessarily restrict the capacity of law enforcement to exchange intelligence and operational information.

1.125 CrimTrac has evolved out of another of the national common police services, the National Exchange of Police Information (NEPI). The announcement of CrimTrac's intended establishment was made by the Prime Minister in October 1998 and in the 1999 Budget some $50 million was committed for its first three years of operation. CrimTrac is a new national crime investigation system which, by using

---

101 NCA, *Annual Report 1999-2000,* pp. 18-19.

102 *Submissions,* p. 81.

103 *Submissions,* p. 133.

state of the art technology, will provide Australia's police with real time access to some of the information they need to make the task of solving crimes more efficient and timely. CrimTrac will include:

- an enhanced National Automated Fingerprint Identification System (NAFIS);
- a new national DNA database; and
- a national Child Sex Offender register, for police use only.

CrimTrac will also provide Australia's police with fast access to operational information including domestic violence orders, person warnings and stolen vehicle information.

1.126 The CrimTrac Agency was established as an Executive Agency under the Commonwealth *Public Service Act 1999* on 1 July 2000 and operates under an intergovernmental agreement signed by all police ministers. Its predecessor - NEPI - now no longer exists. The Agency's work will complement that of the ABCI. While ABCI represents a central intelligence resource, CrimTrac will deliver advanced operational information services and investigation tools to the nation's police. With increasing human mobility between States and Territories, the need for national databases is clear. Importantly, CrimTrac has the formal support of all State and Territory Governments, which will be responsible for contributing to the cost of its administration in the long term.

1.127 NAFIS was first established in 1986 and became one of NEPI's main functions when it was created in May 1990.[104] At that time NAFIS was a world leader in allowing operational officers to match fingerprints held on a central National Database. However, after 13 years of operation, its technology had been overtaken in countries such as Europe, the United States and New Zealand. It was also a relatively slow process. The fingerprinting process involving printers ink, a roller and a slab had barely changed throughout its century of operations. The prints - whether obtained at the station or from the crime scene - had to be posted to NAFIS where they were scanned and searched against the 2.3 million records held in the database. A fingerprint expert then had to verify the match. The poor quality of the prints often thwarted a match.

1.128 CrimTrac's new fingerprint system will make use of the latest livescan technology. Livescan's inkless process uses electronic and laser technology to scan fingers and palm from a flat glass pad to produce a clear and undistorted record. Police officers can then feed the electronic fingerprints to CrimTrac for an immediate search. If they are holding a suspect in custody, such speedy responses will be invaluable.

---

104 Specific details of CrimTrac's operations have been sourced from CrimTrac Factsheets issued by the Attorney-General's Department. See also *Submissions,* pp. 237-240.

1.129 The National DNA Database will similarly revolutionise crime investigation. Australian police have largely relied on DNA evidence in seeking to solve individual cases, by matching DNA taken from a particular suspect to DNA evidence recovered from a crime scene. Two States and the Northern Territory had established their own local DNA databases, which were effective but jurisdictionally limited. DNA evidence has been used to convict persons of offences such as sexual assault, armed robbery and murder, but it has also established the innocence of many others implicated in a crime. The recent mass screening of volunteers in Wee Waa, for example, helped eliminate suspects in a criminal investigation as well as, ultimately, contributing indirectly to a conviction.

1.130 CrimTrac's National DNA Database will contain DNA profiles of existing convicted serious offenders which can be matched against samples obtained from suspects or crime scenes. Because a large number of crimes are committed by a small number of criminals, once criminals have their DNA profile recorded on the database, police will be able to identify them faster. CrimTrac is expected to hold about 25,000 DNA profiles in its first year, with more being added continuously.[105]

1.131 Collection and matching of DNA profiles will be undertaken in accordance with legislation. At the time of writing, the Commonwealth and all States and Territories except Western Australia had passed the necessary legislation to establish the database and to permit DNA samples to be taken from convicted criminals.[106] Despite the legislation having been developed by the Model Criminal Code Officers Committee with the Hon Judge R N Howie QC as its chair, and with input from representatives of all jurisdictions, Mr Cowdery made it clear that the legislation 'struck all the barriers that we are accustomed to between jurisdictions, and it is very frustrating'.[107]

1.132 The world's first national criminal DNA database was established in the United Kingdom in April 1995 and by 1999 held over 500,000 DNA records. Over 10,000 matches had been made between crime scenes and suspects and on average 333 crimes were cleared up per month.[108] More comparable to the Australian federal situation, the United States Federal Bureau of Investigation created a national DNA database in 1998, enabling police to solve multi-jurisdictional crimes, such as of serial rape or murder, where the perpetrator may have moved between states.

1.133 Witnesses to this inquiry from law enforcement, not surprisingly, lauded the development of CrimTrac as a major technological advance in the fight against crime. Emphasis was placed by Dr John Gaudin of Privacy NSW, however, of the need for

---

105 AAP, *Launch of CrimTrac means old cases can be re-examined,* 20 June 2001.

106 The Commonwealth *Crimes Amendment (Forensic Procedures) Act 2001,* Act No. 22, 2001, received assent on 6 April 2001.

107 *Evidence,* p. 170.

108 Report of the Model Criminal Code Officers Committee, *Model Forensic Procedures Bill and the Proposed National DNA Database,* May 1999, p. 1.

high standards of accountability for such database operations in view of their capacity for broad, proactive policing rather than the traditional and more specific investigation of particular offences, which are supervised by judicial officers through warrants and courts exercising their discretion to exclude improperly obtained evidence.[109]

1.134 In its submission, the Victorian Government stressed that its amendments to its *Crimes Act 1958* had, through judicial supervision, ensured an appropriate balance between individual rights and a technology which is regarded by experts worldwide as the most important scientific advance to be offered to the criminal justice system since the development of fingerprint analysis.[110] While Mr Cowdery noted the civil liberties argument that the compulsory acquisition of a person's DNA record is a breach of human rights, he noted that it could be justified by reference to the limited use to which the DNA information could be put - to assist in resolving criminal offending - and that the safeguards contained in the national model legislation assure that the right balance has been struck.[111]

1.135 The Committee strongly endorses the operations of such national databases as a positive means of breaking down the jurisdictional barriers. Not only should Australia seek to remove the protection such jurisdictional barriers provide to criminals, civil liberties are enhanced where such processes confirm innocence as well as guilt. The Committee endorses this comment in the MCCOC report:

> Justice is about getting to the truth, anything that helps in that process should enhance the quality of our justice system.[112]

Laws of evidence

1.136 Several submitters noted that the operations of State and Territory Evidence Acts are also affected by new technology, with the Queensland Minister for Police and Corrective Services in particular pointing to inconsistencies between Commonwealth, State and Territory legislation relating to the preservation of evidence.[113] It would, of course, be a matter of considerable concern to law enforcement if any evidence that had been obtained by use of emerging technology was not accepted as admissible in the courts. As noted above, both Mr Cowdery and Detective Inspector Berriman noted that evidentiary problems may arise when a surveillance device issued under warrant in one jurisdiction moves out of that jurisdiction.[114]

---

109 *Evidence,* p. 134.

110 *Submissions,* p. 139.

111 *Evidence,* p. 173.

112 Report of the Model Criminal Code Officers Committee, *Model Forensic Procedures Bill and the Proposed National DNA Database,* May 1999, p. 4.

113 *Submissions,* p. 91.

114 *Evidence,* pp. 130, 167.

1.137 A representative of ASIC, Mr Keith Inman, informed the Committee that even though ASIC officers operate under a national scheme, they have to take account of the different evidence rules which apply in the jurisdiction in which they are operating.[115]

1.138 The two submissions to this inquiry from Tasmanian Government sources both alluded to the admissibility issue, particularly in relation to photographic evidence obtained by digital imaging and especially for remote devices where there is no evidence from a person who took the photograph.[116]

1.139 NCA witnesses noted that the issue of digital cameras is significant and that there is a fear that electronic data may be more capable of being manipulated than when evidence is in conventional form. They made the point that, at present, courts seem to be willing to accept electronic material in the same way they have traditionally accepted documentary evidence, provided it is properly authenticated.[117]

1.140 In relation to electronic crime, the Attorney-General's portfolio submission noted that:

> The CDPP (Commonwealth Director of Public Prosecutions) can only prosecute cases which involve e-crime if the investigators have the tools they need to properly investigate the alleged offences, collect the evidence needed to prove them and be able to present the evidence in court. This presents a challenge which, while formidable, can be addressed provided that the criminal law, the laws of investigation and the rules of evidence are all kept up to date and are not allowed to lag behind the changing nature of criminal activity.[118]

1.141 The then Western Australian Minister for Police advised the Committee in his submission that admissibility of copies of information obtained under analysis had specifically been one of the issues addressed in a draft Bill prepared in 1999 to tackle computer-based crime in Western Australia.[119]

1.142 In a related matter, the NCA drew attention to the requirement to vary the form and manner in which particularly electronic evidence is presented in court to comply with the laws and procedures of each jurisdiction, while also noting that several jurisdictions have examined their laws of evidence and procedures to permit the greater use of computer facilities in courts.[120] The Committee was advised by the Australian Institute of Judicial Administration of the conduct in October 2000 of a

---

115 *Evidence,* p. 162.

116 *Submissions,* pp. 42-43.

117 *Evidence,* pp. 21-22.

118 *Submissions,* p. 198.

119 *Submissions,* p. 108.

120 *Submissions,* p. 159.

conference entitled 'Technology for Justice 2000' where the use of information technology in support of the administration of justice was discussed. In July 2001 Queensland's University of Technology launched the first purpose-built e-courtroom to help teach law students. Temporary e-courts have hosted cases in the Federal Court and in the Supreme Courts in NSW, Victoria and Western Australia.[121]

1.143 It is clearly only a matter of time before real e-courts are established, as they have been in the United States and Singapore. The Committee notes efforts internationally through the International Organisation of Computer Evidence to establish 'common' computer evidence standards to combat criminal activity that has crossed international borders.[122]

1.144 It again encourages Australian governments to work cooperatively to introduce modernised and harmonised requirements in relation to the admissibility of evidence in the interests of advancing the administration of justice within Australia.

Accountability

1.145 In appropriate contexts elsewhere in this Chapter the Committee has addressed the need for caution in giving law enforcement unfettered access to all the latest technological developments. Some Committee members were troubled by the overall implications for society of the aggregated outcome of the extent and range of intrusive surveillance and database operations of the types discussed, especially when the transition from the physical world to cyberspace is taken into account.

1.146 The issue of the use to which law enforcement might put the ever larger volumes of material it could access in the future was addressed directly by NCA representatives, Marshall Irwin, and Mr Adrien Whiddett, the NCA's General Manager Operations. Mr Irwin noted:

> We appreciate that that is … a live issue and…there is a balance to be drawn… Mechanisms could be built into the process such as already exist in telecommunications interception legislation, for example, and a range of other electronic surveillance legislation, where the intrusion can only occur through the authorisation of a judge or a sufficiently qualified judicial person, and that there be some external overview of the way in which the Authority or any other agency discharges those functions, for example, by extending the role of the Ombudsman or someone similar. I would accept…that any additional powers that agencies were given in this regard would have to be balanced by those types of accountability mechanisms. Obviously, if there were to be judicial approval or a judicial warrant, there would be strict legislative criteria that would have to be complied with before the warrant could be obtained.[123]

---

121 AAP, *Australia's first purpose-built e-court opens,* 4 July 2001.

122 Comprehensive details in *Submissions,* p. 231.

123 *Evidence,* p. 7.

Mr Whiddett added:

> The same [concept] applies for listening devices and telephone interception; in other words, the warrants have been taken out for a good reason and provided by a judge…in the midst of a lot of dross there may only be a few pearls of something interesting. That is the reality at present. There would be a vast amount of material gained by that means, which has no particular interest to the matter in hand but may be of a general nature. It is a question of discerning what is valuable to law enforcement and what is not.[124]

1.147 By way of clarification, Mr Irwin stressed that:

> law enforcement does not have any interest in that sort of information [private and personal] and does not have any interest in trading in that sort of information. It is clearly only interested in that information that advances its investigations in the discharge of its functions.[125]

He added that investigatory material is accorded a high classification at the NCA and that it is breach of the NCA Act for an officer to disclose it other than for the purposes of the Act.

1.148 The AFP submission similarly stressed:

> If the law gives agencies the power to intercept communications, then that power should apply to whatever may in future be considered communications. If legislation is tied to specific technologies, then legislation will have to be rewritten whenever technology advances. The problems being faced now will simply recur.[126]

1.149 The NCA pointed to the existing role of the Commonwealth Ombudsman in oversighting NCA and AFP use of telecommunications interception and the fact that the Ombudman's office had only ever reported a high level of conformance with the provisions of the TI Act, apart from 'minor clerical errors'. This was confirmed by Senior Assistant Ombudsman, Mr Philip Moss:

> …our experience has been that any errors or problems identified during those inspections are quickly addressed and corrected by the law enforcement agencies. As a consequence, our inspections have been instrumental in bringing about changes to the processes that assist in maintaining compliance with the requirements of the TI Act.[127]

1.150 The main thrust of the Ombudsman's submission, as described in para 1.96, was that the current accountability regime is inconsistent. As Mr Moss put it:

---

124 *Evidence,* p. 8.

125 *Evidence,* p. 9.

126 *Submissions,* p. 61.

127 *Evidence,* p. 86.

> The information obtained through a listening device may have a similar content or value to that obtained though telecommunications interception, yet the user of the device is not subject to similar oversight inspection.[128]

The Committee strongly endorses the concept of a consistent accountability regime. It is also important that there is a sound system of independent review of the activities of law enforcement in relation to all use of intrusive measures. Such independent review would provide assurance to the Minister, the Parliament and the public that law enforcement agencies are complying with legislative safeguards with integrity (it is worth noting that the courts will also deal with any illegalities) and respecting citizen's rights.

1.151 In relation specifically to privacy, the NCA submitted that, at all times in carrying out investigations, it is sensitive to privacy implications. Although exempted from the provisions of the *Privacy Act 1988* the NCA seeks to ensure that the collection, use and storage of information is subject to appropriate controls and safeguards. [129] In his submission the Federal Privacy Commissioner, Mr Malcolm Crompton, stressed the importance of privacy to the Australian community but also recognised that finding the right balance between privacy and effective law enforcement does involve complex and difficult judgements. He submitted:

> In looking at future directions in crime prevention including legal and policy responses it is important to recognise that our individual privacy is often taken for granted. Privacy is clearly perceived by Australians as a fundamental human right, and a right we are eager to preserve in a rapidly changing global environment.[130]

1.152 Mr Crompton noted that the impact of crime prevention measures or additional investigative powers will range along a spectrum of privacy intrusiveness and he suggested that the following matters should be considered before additional investigative powers are implemented and granted:

- the power should be conferred, or the measure introduced, expressly, not by implication;
- privacy intrusive powers or measures should be conferred by an Act, not by subordinate legislation;
- the grounds on which power of intrusion may be exercised should be stated expressly and in objective terms;
- the authority to exercise intrusive powers, for example search or seizure should generally be dependent on special judicial authorisation (a warrant); and

---

128 *Evidence,* p. 86.

129 *Submissions,* p. 149.

130 *Submissions,* p. 259.

- other intrusive activities, for example seeking documents using statutory notices or other legislative mechanism, would at least require an appropriately senior officer to authorise the activity.[131]

The Committee strongly endorses these considerations.

1.153 Legal and Policy Officer for Privacy New South Wales, Dr John Gaudin, told the Committee:

> Accountability for the use of intrusive powers requires a greater openness than has often been the case. Law enforcement agencies often argue that people should be prepared to trust their high security and confidentiality standards rather than expect specific measures to deliver accountability. My response is that we cannot assume that powers will not be misused. This is not necessarily restricted to conscious corruption… It can also include overzealousness and impatience with playing by overly formal rules, or the effect of a cultural attitude in law enforcement based on the sense of knowing so much more about the people you are dealing with that you have had the sense of superiority to them.[132]

1.154 Dr Gaudin emphasised that Privacy NSW is concerned about escalating surveillance and, in recognition of the established tradition of judicial warrants to approve intrusive searches, it would wish to see the concept broadened to encompass a 'clear privacy framework' with 'clear legislative safeguards' as new forms of surveillance are approved. He pointed to the absence of any warrant provision over police access to traffic data under the Telecommunications Act as one specific omission in the safeguards structure.

1.155 The Committee notes that the general community appears to have come to accept surveillance as a fact of life, especially as a means of preventing crime. It is in use in the streets, in the shops, in workplaces, in sports stadiums and in casinos. The Wood Royal Commission noted in its report that a March 1997 Morgan-Bulletin Poll had found that 89% of respondents approved of the use of surveillance cameras in public places and 57% in the workplace.[133]

1.156 Similarly, the Federal Privacy Commissioner noted that his Office's research had shown that 57% of respondents would be happy for police to have more access to information on databases if it led to a significant increase in crime prevention. He stressed, however, that the raw data did not adequately reflect people's lack of knowledge and understanding of privacy, and that they may hold different views if they were more aware of how personal information is handled, including for law enforcement purposes. He pointed out that the community probably does have limits to the amount of invasion of privacy it is prepared to bear, such as resisting global

---

131 *Submissions,* p. 267.

132 *Evidence,* p. 134.

133 In *Submissions,* p. 96.

DNA or fingerprinting of whole populations, with its attendant suggestion that we are guilty until proven innocent.[134] As a practical example of such concerns, all samples other than those of the accused were destroyed some five months after the mass DNA sampling undertaken in Wee Waa was completed.[135]

1.157 As the AIIA pointed out in its submission, Governments hold vast amounts of sensitive and personal information and they need to adopt exemplary practices in its management.[136] Thus, the *Commonwealth Privacy Act 1988* contains 11 Information Privacy Principles (IPPs) regulating the collection, storage, use, disclosure and access to, and correction of, one's own personal information by Commonwealth public sector agencies.[137] IPPs 10 and 11 do, however, permit law enforcement use or disclosure of personal information, in recognition that privacy rights must be balanced against other interests, including that the civil rights of the community are helped by maintaining public safety.[138] The Federal Privacy Commissioner noted that these exemptions are included in the Act in recognition that the community clearly wants to be protected from crime, and is willing to concede powers to the law enforcement community.[139]

1.158 In any discussion on expanding police powers, and more specifically in this case in relation to providing law enforcement with the latest technological tools with which they can catch criminals, a delicate balance has to be struck between the privacy rights of citizens and the public interest in maintaining law and order in our community. The Committee has already made recommendations in relation to the issue of the appropriate legislative response and which include full and proper accountability measures. It remains necessary only to make a specific recommendation in relation to the need for the role of the Ombudsman to be expanded in the interests of a consistent approach to accountability.

Recommendation 8: That the Commonwealth Ombudsman's jurisdiction over the use by Commonwealth law enforcement agencies of telecommunications interception be expanded to include the use of any electronic surveillance device.

Conclusions

1.159 New technology is unquestionably a major aid to both criminals and law enforcement services alike. The rapid advance of technology now sees the traditional police officer on patrol in a high-powered car with portable radios and all manner of sophisticated paraphernalia - a far cry from the helmet, whistle and truncheon

---

134 *Submissions,* p. 262.

135 AAP, *Wee Waa's DNA samples go up in smoke,* 20 September 2000.

136 *Submissions,* p. 71.

137 The Victorian Government submission drew attention to its Information Privacy Bill 2000 which was to establish a similar scheme of regulation of the use of personal information in the Victorian public sector - *Submissions,* p. 140.

138 Attorney-General's portfolio, *Submissions,* pp. 195-196.

139 *Submissions,* p. 262.

possessed of an officer 'on the beat' in the not so distant past. At the Customs barrier, traditional methods of manual observation and drug-detecting sniffer dogs have been supplemented by 'Backscatter' X-ray technology, Ionscans and K910B Buster devices.[140] It is clear that such developments in the use of technology are a positive aid to crime control. The prospects for the future are limited only by human ingenuity, with cost reductions, miniaturisation and increasing connectivity offering the benefits of ubiquity and speed.

1.160 Equally persuasive is the argument that if the public and governments have an expectation that their law enforcers will investigate and bring to justice the perpetrators of serious crime, then they should be given access to the latest investigatory tools. Obviously adequate funding holds part of the answer - an area outside the Committee's area of interest. It can, however, give advice to governments about the adequacy of the legislative environment that they have created and in which their officers are expected to operate with maximum effectiveness.

1.161 This Chapter has highlighted the inconsistencies in the national legislative structure which act to thwart efficient law enforcement but which criminals are free to exploit. While in recent years Australian governments have achieved much for which they should be commended, with the development of CrimTrac the most notable example, the Chapter contains a clear call to the Commonwealth, State and Territory Governments to work together on achieving outcomes which are beneficial for all Australians, not simply parochial local interests.

1.162 With goodwill on all sides, positive progress was able to be made in the comparable area of the national regulation of corporations. Harmonisation of State and Territory laws does not require total uniformity, only consistency. That is indeed the basis on which the Committee can call for consideration to be given for TI to be devolved to the States on the one hand without being in contradiction on the other hand with its general proposition that cross-border differences should be eliminated in relation to surveillance device legislation. It may well be, therefore, that the national classification system holds a better precedent for a national law enforcement regime, where all parties have agreed to abide by common national standards, while individually retaining discretion over offence provisions at the State and Territory level. New and emerging technological developments raise many challenges. Governments must meet those challenges cooperatively and proactively.

---

140 See *Submissions,* pp. 202-3 and 241 for detailed descriptions. Mrs Marion Grant, the Australian Customs Service's National Manager, Border Operations, also informed the Committee that a cargo management re-engineering process was underway to make greater use of computer applications, including artificial intelligence systems, in its dealings with importers and exporters - see *Evidence,* p. 54.