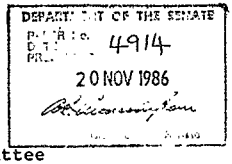
The Parliament of the Commonwealth of Australia



Report of the Joint Select Committee on Telecommunications Interception

November 1986

The Parliament of the Commonwealth of Australia

Report of the Joint Select Committee on Telecommunications Interception

November 1986

TABLE OF CONTENTS

Throughout the inquiry, the Committee received un-reserved co-operation from two key Commonwealth agencies, the Australian Federal Police and the Australian Telecommunications Commission. State Police forces permitted by their Governments to make submissions to, and appear before, the Committee made a significant contribution. The Committee is grateful to these organisations, and extends its thanks also to the various law societies, police associations, civil liberties groups, Government departments and private individuals who gave evidence to the Committee or made submissions.

The Committee was surprised at the response of State Governments to invitations to contribute to the Committee's inquiry. Their responses are detailed in the report, and can best be described as less than enthusiastic, particularly when the main issue before the Committee involved a significant potential devolution of Commonwealth power to the States.

Most of the issues raised by the inquiry involved the Committee in 'drawing the line' between conflicting, and, occasionally, opposing positions. Balanced judgments were required, and in large measure, the Committee achieved agreement. The Committee trusts that the report contributes to public awareness and discussion of the issues involved, and assists in the development of appropriate legislation in this important and sensitive field.

(S P Martin, MP)
Chairman
20 November 1986

PREFACE

The Joint Select Committee on Telecommunications Interception sat for the first time on 17 July 1986 and for the last time on 18 November 1986. In that 4 month period, the Committee was required to examine and report on firstly, the Telecommunications Interception (Amendment) Bill 1986, and, secondly, the recommendation contained in Mr Justice Stewart's Report of the Royal Commission of Inquiry into Alleged Telephone Interceptions to the effect that the power of interception be extended to cover all serious offences.

The Committee was unique in the history of the Parliament, this being the first occasion since Federation that a Bill originating in the House of Representatives has been referred to a joint select committee for examination and report. The Bill itself is complex, and covers an area in which there is a wide divergence of views within the community and within the Parliament.

The Committee took the view that it should, in accordance with its resolution of appointment, present a final report to the Parliament as soon as possible. A target for reporting, November 1986, was set by the Committee at its first meeting. This target precluded a protracted inquiry into peripheral issues raised by a consideration of the Bill and in evidence taken by the Committee.

The issues central to the Committee's inquiry were, however, examined in detail. These included:

a. the requirement of law enforcement agencies to have rapid access to information which would assist in countering organised and drug-related crime and in solving other serious criminal offences;

b. the protection of individual privacy from unwarranted intrusion;

c. the prevention of abuse of interception powers;

d. the protection of the integrity of the telecommunications system;

e. the need for a thorough and practicable system of safeguards, consistent with administrative efficiency;

f. the requirement for a streamlined system for the lawful implementation of interceptions;

g. the admissibility of evidence gained through legal and illegal interceptions;

h. the communication of information gained through legal interceptions, and

i. the problems created by the free availability of devices capable of effecting illegal interceptions.

Throughout the inquiry, the Committee received un-reserved co-operation from two key Commonwealth agencies, the Australian Federal Police and the Australian Telecommunications Commission. State Police forces permitted by their Governments to make submissions to, and appear before, the Committee made a significant contribution. The Committee is grateful to these organisations, and extends its thanks also to the various law societies, police associations, civil liberties groups, Government departments and private individuals who gave evidence to the Committee or made submissions.

The Committee was surprised at the response of State Governments to invitations to contribute to the Committee's inquiry. Their responses are detailed in the report, and can best be described as less than enthusiastic, particularly when the main issue before the Committee involved a significant potential devolution of Commonwealth power to the States.

Most of the issues raised by the inquiry involved the Committee in 'drawing the line' between conflicting, and, occasionally, opposing positions. Balanced judgments were required, and in large measure, the Committee achieved agreement. The Committee trusts that the report contributes to public awareness and discussion of the issues involved, and assists in the development of appropriate legislation in this important and sensitive field.

(S P Martin, MP)
Chairman
20 November 1986

MEMBERS OF THE COMMITTEE

Chairman:	Mr S.P. Martin, M.P.
Deputy Chairman:	Mr P.M. Ruddock, M.P.
Members:	Senator B.R. Archer
	Senator J.R. Black
	Senator B. Cooney
	Senator D.B. Vigor
	Hon. P. Duncan, M.P.
	Mr M.J. Lee, M.P.
	Mr P.J. McGauran, M.P.
Secretary:	Mr P.N. Gibson, M.C.
Committee Secretariat Staff:	Ms D.M. Miles
	Ms K.E. Crouch
	Mrs Y.M. Huddleston

TERMS OF REFERENCE

1. In June 1986 the Parliament of the Commonwealth of Australia established the Joint Select Committee on Telecommunications Interception to examine and report upon:

(a) the Telecommunications (Interception) Amendment Bill 1986, and in particular, the appropriateness of the mechanism for conducting interceptions and the safeguards for their authorisation, recording, transcribing, dissemination and retention, and

(b) the recommendation contained in Mr Justice Stewart's report of the Royal Commission of Inquiry into Alleged Telephone Interceptions to the effect that the power of interception be extended to cover all serious offences.

THE CONDUCT OF THE INQUIRY

1. The Joint Select Committee on Telecommunications Interception was established by resolution passed by the House of Representatives on 4 June 1986 and by the Senate on 13 June 1986. The Committee held its inaugural meeting on 17 July 1986, elected a Chairman and resolved to complete the inquiry and report to the Parliament by the end of November 1986.

2. On 25-26 July 1986 the Committee advertised nationally, inviting submissions. 44 submissions were received, largely from State Police Forces and Associations, the Australian Federal Police, the National Crime Authority, Telecom Australia and Civil Liberties Organisations. A number was also received from the general public and organisations representing a diverse range of interests. A list of submissions is contained in Appendix I.

3. Between August and October 1986, the Committee conducted inspections and took evidence at hearings. 31 exhibits were incorporated in the Committee's records. A list of exhibits is contained in Appendix II.

4. A wide range of individuals and organisations was given the opportunity to put their views on telecommunications interception to the Committee. Specific invitations were sent to relevant Federal Ministers, the State Premiers and the Chief Minister of the Northern Territory. Federal Ministers to respond included the Attorney-General, the Special Minister of State, the Minister for Aviation and the Minister for Communications. Submissions were received from the Governments of Queensland and South Australia.

5. The Committee sat on 17 occasions and took evidence from 37 witnesses at public hearings. The transcript of evidence totalled 1101 pages. Hearings were held in:

- Canberra - 25 August 1986
  - 24 October 1986
- Melbourne - 2,3 and 29 September 1986
- Sydney - 4 and 30 September 1986

6. A list of the witnesses who gave evidence at the hearings is contained in Appendix III.

SUMMARY OF MAJOR CONCLUSIONS AND RECOMMENDATIONS

	Conclusions and Recommendations	Paragraph No
1.	With respect to the Telecommunications Interception (Amendment) Bill 1986 the Committee concludes that:	
	a. the Bill is confusing, convoluted and vague in parts, compounding difficulties created by legislation which is already overly complex;	2.100-2.107, 6.3-6.8
	b. the safeguards proposed by the Bill are inadequate;	2.116-2.127, 2.164, 6.36-6.56
	c. difficulties in interpretation are created by the use of terms in the Bill which are either inadequately defined or are unknown in existing State legislation, and	2.41-2.48, 2.154
	d. the scope of the proposed legislation is insufficiently defined and does not fully explore the implications of developing technologies and the growth of non-verbal information transmissions.	2.49-2.54, 2.155
2.	With respect to the Telecommunications Interception (Amendment) Bill 1986, the Committee recommends that:	
	a. the Bill be withdrawn, and	3.47,6.19

b. there be substituted for the subject Bill a Bill for an Act to consolidate and re-structure the principal Act, incorporating applicable provisions of the subject Bill and the recommendations contained in this report. 6.19

3. With respect to the proposed extension of interception powers to the States of the Commonwealth, the National Crime Authority and the NSW Drug Crime Commission, the Committee concludes that:

a. there is a requirement for information from telecommunications interception to be extended so that the State and Northern Territory Police forces, the NCA and the NSW Drug Crime Commission have rapid access to information on serious drug crimes; 3.46

b. the case to extend to the NCA, State and Northern Territory Police forces and the NSW Drug Crime Commission the power to intercept telecommunications has not been made; 3.46

c. that essential rights to privacy and the protection from illegal intercepts and the malicious use of intercepted material are best preserved by restricting to the minimum the number of agencies legally empowered to effect interception; 3.46

d. each law enforcement agency should retain the full power to select targets, determine priorities, appraise Telecom, prepare draft warrants and approach Federal Court Judges seeking the issue of the warrants, and 3.46

e. that while the legal right to target interceptions should be extended and decentralised, once the warrant is issued the interceptions should be carried out by a single agency, on a regional basis if economically justified. 3.46

4. With respect to the proposed extension of interception powers to other agencies, the Committee recommends that:

a. a Telecommunications Interception Agency be established to carry out all interceptions for the AFP, the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission; 3.46

b. all intercepts should continue to be made through Telecom; 3.46

c. the Telecommunications Interception Agency should be established within the AFP as it is best placed to conduct the interceptions for all authorised agencies, and can guarantee a career structure for officers and maximum staff turnover; 3.46

d. the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission should each be offered lines for telecommunications interception on a full cost-recovery basis and each law enforcement body should have the power to determine the priorities for use of the lines rented, and 3.46

e. this extension of access to intercepted information to the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission must be accompanied by stringent centrally co-ordinated safeguards, recognising at the same time a requirement for administrative efficiency and the need for a fast-track mechanism for urgent interceptions to exist with subsequent justification. 3.46

5. With respect to the extension of interception powers to cover serious offences, as recommended by Mr Justice Stewart, the Committee concludes that:

a. a case has been made for law enforcement agencies to have ready access to intercepted information in only the most serious offences, as well as serious drug trafficking offences; 4.39

b. the number of serious offences for which intercepted information should be available should be kept to the absolute minimum, and 4.39

c. serious offences should be defined in the Act. 4.39

6. With respect to the extension of interception powers to cover serious offences, the Committee recommends that:

a. if the incident and nature of offences gives rise to community concern that interception powers ought to be extended to cover further offences, this should be reflected by a further amendment to the proposed Act by Parliament, and 4.39

b. until Parliament otherwise provides, serious offences defined in the proposed Act should be restricted to only the following offences, hereinafter referred to as 'relevant offences':

(i) murder;

(ii) kidnapping, and

(iii) organised crime associated with offences:

(a) that involve 2 or more offenders and substantial planning and organisation and

(b) that involve, or are of a kind that ordinarily involve, the use of sophisticated methods and techniques and

(c) that are committed, or are of a kind that are ordinarily committed, in conjunction with other offences of a like kind and

(d) that involve kidnapping, murder or serious drug trafficking offences and associated financial dealings in each case,

or which relate to conspiracy to commit any of the above offences. 4.39

7. With respect to the problem of illegal interception, the Committee concludes that:

a. the extent of illegal interception would be lessened if the availability of devices designed solely for telecommunications interception purposes were substantially reduced; 5.23-5.25

b. widespread advertising of potential interception devices encourages a disregard for the law, and 5.23-5.25

c. the range of illegal interceptions must be reduced. 5.23-5.25

and the Committee recommends that:

a. devices designed solely for effecting interceptions be declared prohibited imports, subject to control by Government licence for specific law enforcement purposes only; 5.23-5.25

b. the manufacture, importation, advertising, sale and possession, installation and use of such devices be made illegal, and subject to penalties in accordance with those prescribed for physically effecting interceptions, and 5.23-5.25

c. Telecom actively pursue the maintenance of the integrity of the network and the detection of illegal devices as a matter or urgency. 5.23-5.25

8. Concerning safeguards necessary in legislation to replace the subject Bill, and the Act, and related matters, the Committee concludes that:

a. the present safeguards applying to the Australian Security Intelligence Organisation are satisfactory; 6.37

b. authority to issue warrants to intercept should be restricted to Judges of the Federal Court of Australia, for a maximum life span of 90 days; 2.153, 6.40

c. before granting warrants, Judges should be satisfied that: 6.40

(1) there are reasonable grounds for suspecting that the nominated telephone service is being, or is likely to be, used by a person who is suspected, on reasonable grounds, of

(a) committing;

(b) having committed;

(c) being about to commit, or

(d) conspiring to commit

a relevant offence;

(2) other investigative techniques have either been exhausted or would, in the circumstances, be inappropriate, and

(3) information likely to be obtained from the warrant would materially assist in the investigation of a relevant offence that the person is suspected, on reasonable grounds, of

(a) committing;

(b) having committed;

(c) being about to commit, or

(d) conspiring to commit

d. warrant applications should specify: 6.41

(1) the identity of the law enforcement officer applying for a warrant, and the identity of the authorising officer;

(2) a statement of the time for which an interception is sought, and a justification for any application extending to the maximum warrant period of 90 days, with a statement establishing why the interception of successive communications is considered necessary, and

(3) a statement of previous interceptions sought or effected which involved the same person, telephone service or place, with the results of such interceptions.

e. a 'fast-track' mechanism should exist, to enable a Judge to issue a warrant by telephone, but only in the most urgent circumstances, followed by full sworn information provided within one working day; 6.42

f. legal professional privilege must be protected; 6.44

g. the Commonwealth Attorney-General must be satisfied as to the adequacy of complementary State/Northern Territory legislation before prescribing, by way of regulation, an agency of a State/Territory to be authorised to initiate warrants for interception, 6.45

h. warrant provisions for the initiation of telecommunications interceptions by the AFP and the NCA should be identical, should be no less stringent than those applicable to other agencies, should not authorise any entry on premises and should be effected through Telecom alone. 6.43, 6.48

9. In respect of revised legislation covering telecommunications interception and related issues, the Committee recommends that:

a. the Commonwealth, through enacting model legislation for the ACT to regulate the use of listening devices, should encourage uniformity of approach and standards between the States in the use of such devices; and 6.19

b. the communication of any legally intercepted information other than that requested by warrant should be prohibited, unless it relates to an offence punishable by imprisonment for 3 years or longer (there should be no exceptions to this provision.); 6.51

c. penalties for misuse of legally obtained information from interceptions should be at least as stringent as those applicable to offences related to illegal interceptions, except for technical breaches; 6.52

d. reporting provisions on the nature and extent of intercepts effected should be strengthened and extended, and 6.53, 6.54

e. a judicial auditor should be appointed to provide independent audit and scrutiny of the implementation of interception procedures in their totality, excluding those conducted by the Australian Security Intelligence organisation. 6.65

f. the recommendations in this report should be effected as a matter of urgency. 6.19

CHAPTER 1

THE BACKGROUND TO THE INQUIRY

Introduction

1.1 The release in May 1986 of Mr Justice Stewart's Report of the Royal Commission of Inquiry into Alleged Telephone Interceptions was the principal catalyst in the chain of events leading to the establishment of the Joint Select Committee on Telecommunications Interception. On 1 May 1986, the Attorney-General presented Volume One of Mr Justice Stewart's Report in the House of Representatives. In so doing, he observed that the Government was 'in the final stages of a Bill to amend the Telecommunications (Interception) Act following decisions made at the special Premiers meeting on drug strategy in April 1985 ... Mr Justice Stewart's recommendations will be urgently considered in the context of that proposed legislation'.[1]

1.2 On 4 June 1986, the Attorney-General presented the Telecommunications (Interception) Amendment Bill 1986. The Bill was read a first time, and the Attorney-General moved for its second reading. In this speech, he said that:

> The Government now believes that the questions arising from an extension of telecommunications interception powers for law enforcement purposes, including whether such powers should be extended beyond drug offences, call for thorough parliamentary consideration. For that reason, I shall be moving a resolution to establish a joint select committee to examine and report on the Bill, with particular emphasis on the question of extending the interception powers to cover serious offences, on the appropriateness of the proposed legislative safeguards and controls and on the feasibility of having a central Commonwealth agency to carry out interceptions for other authorities.[2]

1.3 The Attorney-General then moved that the Bill be referred to a joint select committee for examination and report. In speaking to this motion, the shadow Attorney-General indicated that, although the Opposition opposed in principle the Bill's reference to a joint select committee, the Opposition would nevertheless participate in the Committee's work.

1.4 The resolution establishing the Committee was passed by the House of Representatives on 4 June 1986 and by the Senate on 13 June 1986. The Senate was informed of the nomination of Senators to serve on the Committee on 13 June 1986. In letters from the Parties, the Speaker of the House of Representatives was informed of the nomination of Members during June 1986. The Committee held its inaugural meeting on 17 July 1986, elected a Chairman and decided on an inquiry program of public hearings and private meetings, with the aim of presenting its final report to the Parliament as soon as possible, and certainly by the end of November 1986.

Australian Federal Interception Legislation - A History

1.5 Although the Constitution clearly gave the Parliament of the Commonwealth the power to legislate with respect to telephonic services, it was not until 1960 that federal legislation covering telephonic interceptions was considered necessary. A brief outline legislative history of federal interception is in the following paragraphs.

1.6 Telephonic Communications (Interception) Act 1960. The essential aspects of this legislation were:

a. to prohibit interception of telephonic messages in their passage over the telephone system except in the performance of normal duties within the Postmaster-General's Department or pursuant to a warrant issued by the Attorney-General to the Australian Security Intelligence Organisation, and

b. to prohibit communication of intercepted information except in defined circumstances.

1.7 There were no significant amendments to the 1960 Act until it was repealed and replaced by the Telecommunications (Interception) Act 1979 which:

a. prohibited interception of any communication passing over a telecommunications system except in performance of normal duties by officers of the Australian Telecommunications Commission (Telecom) or purusant to a warrant issued by the Attorney-General to the Australian Security Intelligence Organisation (ASIO) or by a Judge to Customs (now the Australian Federal Police - AFP) in relation to a narcotics offence (before this, there was, no legislative provision for telecommunications interception in relation to drug offences);

b. provided for issue of warrants for ASIO or Customs (AFP) to intercept telegrams, and

c. prohibited communication of intercepted information except in defined circumstances.

The Royal Commission of Inquiry into Alleged Telephone Interceptions

1.8 The Royal Commission of Inquiry into Alleged Telephone Interceptions (referred to in the following paragraphs as 'the Stewart Royal Commission', 'the Commission' or 'Stewart', as appropriate) was established by Letters Patent of the Governor-General on 29 March 1985 and of the Governor of New South Wales on 3 April 1985. Complementary Letters Patent were issued by the Governor of Victoria on 17 June 1985.

1.9 The key Commonwealth aspects of the Commission's inquiry, in terms relevant to this Committee's inquiry, were to inquire and report:

a. whether there existed, in the possession of any person (including any member of the New South Wales Police Force or the Australian Federal Police), any information or material (including documents or tape recordings) arising out of or relating to the unlawful interception, on or before 28 March 1985, in New South Wales of communications passing over a telecommunications system, being information or material that disclosed the commission of criminal offences or the possible commission of criminal offences against a law of the Commonwealth or of a Territory and which warranted further investigation;

b. on the nature of the offences or possible offences disclosed by information or material referred to above, and

c. on the extent to which documents were given or information communicated pursuant to sub-section 7BA(4) of the Telecommunications (Interception) Act 1979.

1.10 The Commonwealth Letters Patent further contained the following critical requirement:

> AND We require you to make such further recommendations arising out of your inquiry as you think appropriate, including recommendations as to the method of enforcement of the criminal law and the legislative or administrative changes (if any) that are necessary or desirable in the light of the results of your inquiry.[3]

1.11 The Commissioner took evidence for 49 days, between 24 May 1985 and 19 December 1985. All hearings were held in Sydney. 173 witnesses were examined. The transcript of evidence taken came to 3984 pages, and there were 237 documentary exhibits.

1.12 At the conclusion of his inquiry, Mr Justice Stewart made 12 major recommendations. These were as follows (with those germane to this Committee's inquiry being highlighted);

a. that amendments to legislation to extend the power to conduct telephone interceptions to police forces of the States and Territories and the National Crime Authority, be made as soon as possible;

b. that the legislative limitations on the use of telephone interceptions to drug trafficking offences only be removed;

c. that the power to issue warrants be restricted to Judges of the Federal Court and of Supreme Courts of the States or Territories;

d. that the Act be further amended to give a discretion to a Judge to authorise telephone interceptions by warrant after considering:

(1) the gravity of the matters being investigated;

(2) the extent to which the privacy of any person is likely to be interfered with, and

(3) the extent to which the prevention or detection of the crime in question is likely to be assisted.

e. that in appropriate cases the Judge issuing a warrant should authorise an interception to be made directly by a mobile unit without recourse to Telecom. This should apply to the AFP as well as State and Territory police forces and the National Crime Authority;

f. that a review of the present system of interceptions used by the AFP be undertaken with a view to making it more efficient;

g. that State Police should be empowered to make interceptions in their State independently of the AFP system;

h. that the Act be further amended to make it an offence to possess, communicate, divulge or record information obtained by unlawfully intercepting a telecommunication;

i. that admissibility of such material should be determined by the Common Law;

j. that legislation should provide that it is not an offence for police or other relevant persons or authorities to possess, use or copy material which is the produce of illegal interceptions. The relevant persons and authorities would be those mentioned in section 6P of the Royal Commission Act 1902 and persons under their control;

k. that all records in possession of the Commission upon its cessation be passed into the custody of the Chairman of the National Crime Authority. An amendment to the National Crime Authority Act may be necessary to effect such a transfer of records

although it may be considered that the provisions of section 22(3) of the Archives Act 1983 could be utilised to vest custody of this material in Mr Justice Stewart as Chairman of the National Crime Authority on and from the date of the conclusion of his Commission, and

1. that it be an offence to sell or advertise for sale electronic devices designed for effecting telephone interceptions; devices being made prohibited imports.[4]

Present Legal Australian Telecommunications Interception Practices

1.13 The legal framework against which ASIO and the AFP may at present legally intercept telecommunications is provided by the Telecommunications (Interception) Act 1979. The philosophical intent of the legislation is made quite clear by section 7:

> 7.(1) A person shall not -
>
> (a) intercept;
>
> (b) authorize, suffer or permit another person to intercept; or
>
> (c) do an act or thing that will enable him or another person to intercept,
>
> a communication passing over a telecommunications system

1.14 The purpose of the legislation was to prohibit interception. However, it continued the power granted to ASIO in the 1960 legislation to effect interceptions under stipulated conditions in matters relating to national security. It also gave to the Department of Customs the power to intercept in relation

to narcotics offences. In late 1979, the Australian Federal Police was substituted for the Department of Customs following the disbanding of the Federal Narcotics Bureau.

1.15 Before examining in detail the procedures used by ASIO and the AFP in conducting legal interceptions, it is appropriate to consider briefly the extent to which legal interception is currently conducted in Australia. The AFP told the Committee in evidence that it 'has the capacity in terms of available equipment to monitor 38 telephones. However, staffing and financial constraints and experience have effectively limited monitoring to an average of 15 intercepts at any one time.'[5] The Committee did not wish to prejudice ASIO's activities by asking directly for a similar answer, but the Director-General of Security told the Committee in evidence that 'the level of intercept capability that we have is of the same order as that of the police.'[6]

1.16 The Australian Security Intelligence Organisation (ASIO). The Director-General of Security, Mr A.K. Wrigley, gave evidence to the Committee on the procedures through which ASIO's interceptions are currently effected under the principal Act. Mr Wrigley began his evidence by giving a general background:

> Firstly, the basis for telephone intercept proposals within ASIO is the framework of an intelligence collection program which is an annual planning framework that we develop. With very few exceptions, a telephone intercept by ASIO is not an impulse or short term planning thing; it is part of a long term program to collect intelligence in designated areas. Proposals for intercept are initiated only where the objectives are regarded as a substantial priority, and only where we would expect to get valuable information from the intercept which would not be obtainable by less intrusive means.[7]

1.17 The Committee was advised that, as with most ASIO activities, a requirement for interception is initiated within ASIO's regional offices. A regional director, when satisfied with a proposal in specific terms, sends it to ASIO's headquarters, where it is reviewed by the relevant intelligence analysis branch. If the proposal is accepted at that stage, it is forwarded to a group chaired by the Deputy Director-General, the Operational Resources Group. This group considers a proposal for soundness, necessity and appropriateness, prior to the drafting of a warrant.

1.18 The draft warrant, the Committee was told, is then considered, with associated relevant documents, by the Director-General. If approved, the draft is covered by a 'request for warrant' document and sent for consideration by the Attorney-General.

1.19 An approved warrant enables ASIO to liaise with Telecom to effect an interception. After an intercept is connected, traffic is routed to ASIO where it is either monitored directly or recorded for later analysis. Each monitor works to an intercept brief, which means that only material relevant to the brief is transcribed. A rough transcript is prepared and passed for preliminary analysis. This determines if a complete transcription and a more detailed analysis are necessary. All transcripts are held within a restricted registry with limited access, where they form part of collated material for the development of intelligence assessments.

1.20 Mr Wrigley further advised the Committee that, as each warrant expires, the Director-General is required to advise the Attorney-General of the results of the interception. ASIO's warrants may remain in force for up to six months under current legislation.

1.21 The Australian Federal Police (AFP). The Committee took evidence from representatives of the AFP at the start of its inquiry. In their submission to the Committee, the AFP stressed the essential nature of interceptions in the successful conduct of their inquiries:

> The interception of telecommunications is an invaluable aid in the investigation of narcotic related crimes; an aid to be used to assist the AFP to attain its first priority, when normal policing methods and good investigatory techniques will not suffice.
>
> The importation of drugs into Australia, in most instances, involves detailed planning by financiers, organisers, overseers, couriers and distributors, who must enter into conspiratorial activity in order to achieve their objective. Telecommunications interception material provides invaluable intelligence regarding these activities and is usually the only admissible evidence of the association between the conspirators. This evidence is essential in proving offences of conspiracy to import and distribute illicit drugs. When use of traditional investigatory methods has been exhausted, telecommunications interception can be the only method of obtaining the information or evidence required.
>
> There are many instances where material gained by the AFP as a result of telecommunications interceptions has been of immense value and would not have been available from any other source. Telecommunications interception has also provided practical evidence of other offences, including official corruption, and such evidence has been lawfully communicated to other law enforcement agencies.[8]

1.22 The procedures followed by the AFP in effecting lawful interceptions were drawn together by Mr Justice Stewart in Chapter 15 of his Report.[9] In summary, these procedures are as follows:

a. after traditional investigative methods have been fruitless, and if the technique is appropriate, the senior investigator prepares a detailed brief, supported by a draft affidavit and warrant;

b. the regional AFP commander assesses the application for a warrant, and, if appropriate, recommends it for further assessment by the AFP Special Projects Committee in Canberra;

c. the Special Projects Committee considers the application against overall national priorities and resources available. Checks are also made, according to evidence taken by Stewart, 'to verify the accuracy of the details provided for the particular telephone service to which the interception device is to be connected and the documents are checked to ensure compliance with the provisions of the Act.'[10]; and

d. once approved by the Special Projects Committee, the applicant then, with assistance from the office of the Director of Public Prosecutions, approaches a judge seeking the issue of a warrant.

1.23 After a warrant is issued, the AFP Special Projects Branch gives advance notice to Telecom HQ by telephone, and written notice is prepared. At the same time, formal advice is prepared, for the Commissioner's signature, to the Attorney-General and the Special Minister of State. A certified copy of the warrant and formal notification are hand-delivered to the Telecom HQ liaison officer responsible for facilitating interceptions.

1.24 The recording procedure for interceptions by the AFP were summarised in the AFP submission as follows:

> The recording of an intercepted telecommunications service commences once advice is received, from Telecom, that the warrant has been received and checks made to ensure the correct service is connected.
>
> Recordings are currently carried out by way of reel to reel tape recorders (master copy) and a cassette recorder (working copy). Call date, duration and number called are recorded on a dialled number recorder/indicator.
>
> The master copy is recorded on specially modified equipment which records very slowly, thereby increasing recorder capacity.
>
> The working copy is used to determine relevance of communication as well as for transcription and any necessary dissemination.
>
> All intercepted telecommunications services are as far as possible monitored at the time of recording and a log sheet is completed and initialled by the monitor noting the date and time and the counter number at the start and completion of the call, together with an indication of the contents of the conversation monitored.[11]

1.25 As part of its submission, the AFP included a document entitled 'Telecommunications Interception Policy', which details AFP responsibilities in all aspects of its interception procedures. The document, prepared in August 1985, impressed the Committee as a detailed statement of various responsibilities in the different stages of effecting interceptions. It is reproduced as Annex A to this Chapter, as the Committee believes that it may form a planning basis for any other agency which may in the future be empowered to effect telephone interceptions.

Selected Overseas Interception Practices

1.26 At its second deliberative meeting, the Committee decided that it would be of value to seek comparative information on interception practices from selected countries with either comparable political, legal or democratic values or systems. Accordingly, information was sought from the High Commissions of the United Kingdom and Canada and the Embassies of France, Sweden and the United States. Specifically, information on the following areas was sought:

a. *legislation governing the interception of* communications;

b. legislative explanatory memoranda or other background documents;

c. relevant Government White Papers or their equivalent, and

d. relevant Law Reform Commission reports, where applicable.

1.27 The High Commission of the United Kingdom and the Embassies of Sweden and the United States responded very fully, and the Committee is most grateful. Subsequent paragraphs summarise the outline position in these countries and the *following documents have been included in the Committee's public* records as Exhibits:

a. United Kingdom (Exhibit 23)

(1) Report of the Committee of Privy Councillors appointed to enquire into the interception of communications ('The Birkett Report') dated October 1957;

(2) Paragraphs 14-18 of the Report of the Committee of Privy Councillors appointed to enquire into 'D' Notice matters ('The Radcliffe Report') dated June 1967;

(3) 'The Interception of Communications in Great Britain', dated April 1980;

(4) 'The Interception of Communications in Great Britain', (report by the Rt Hon Lord Diplock) dated March 1981;

(5) 'The Interception of Communications in the United Kingdom', dated February 1985, and

(6) The Interception of Communications Act 1985.

b. United States (Exhibit 24)

(1) Chapter 119 - 'Wire Interception and Interception of Oral Communications' - 18 United States Code Sections 2510-2520, pp 536-551;

(2) Report 99-647, House of Representatives, 99th Congress, 2nd Session, Report from the Committee on the Judiciary on the Electronic Communications Privacy Act of 1986;

(3) Statement of James Knapp, Deputy Assistant Attorney-General, Criminal Division, to the Committee on the Judiciary, 5 March 1986;

(4) 'Report on Applications for Orders Authorising or Approving the Interception of Wire or Oral Communications (Wiretap Report)', for the period 1 January 1985 to 31 December 1985, Administrative Office of the US Courts, April 1986; and

(5) Extract from Congressional Record - House, 23 June 1986.

c. Sweden (Exhibit 25)

(1) The Swedish Code of Judicial Procedure, Report No 16, the National Council for Crime Prevention, Sweden, May 1985.

1.28 At the further request of the Committee, the Attorney-General's Department provided a summary of relevant legislation in Canada, the United Kingdom, and the United States.[12] This material is used in the paragraphs that follow together with material from Chapter 15, Mr Justice Stewart's Report.

Canada

1.29 Part IV.I of the Canadian Criminal Code prohibits the interception of 'private communications' (any oral communication or any telecommunication made in circumstances where privacy could be reasonably assumed) except for law enforcement purposes pursuant to a judicial authorization and in certain other defined circumstances. (Interception for national security purposes is dealt with by other legislation). Part IV.I also prohibits the disclosure of private communications except in specified circumstances and prohibits the possession of equipment for the purpose of intercepting private communications.

1.30 The legislation lists a number of offences under the Criminal Code and other federal statutes in connection with which interception may be authorised. These offences include treason, sabotage, forgery, hijacking, firearms and explosives offences, bribery, corruption, obstructing justice, murder, assaults, kidnapping, advocating genocide, fraud, breaking and entering, arson, gaming and betting, drug offences and smuggling.

1.31 An application for a judicial authorization must be signed by the Attorney-General of the province in which the application is made or the Solicitor-General of Canada or a specially designated official and must be accompanied by an affidavit deposing to certain matters, including:

a. the facts relied upon to justify the belief that the authorization should be given together with particulars of the offence;

b. the type of private communication proposed to be intercepted;

c. the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable and probable grounds to believe may assist the investigation of the offence;

d. the number of instances, if any, on which an appliction has been made under the Code in relation to the offence and any person named in the affidavit and on which the application was withdrawn or no authorization was given;

e. the period for which the authorization is requested, and

f. whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

1.32 An authorization may be given if the judge to whom the application is made is satisfied:

a. that it would be in the best interests of the administration of justice to do so, and

b. that other investigative procedures have been tried and have failed, or are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

1.33 An authorization is required to state the offence in respect of which communications may be intercepted; the nature of those communications; the identity of the persons, if known, whose communications are to be intercepted; and may contain such terms and conditions as the judge considers advisable in the public interest. An authorization is valid for the period specified therein which cannot exceed 60 days.

1.34 Special provision exists for emergency authorizations. The legislation also contains provisions for keeping all documents relating to an application secret, by placing them in a sealed packet to be kept in the custody of the court, and to be opened only for the purpose of dealing with an application for renewal or pursuant to an order of a judge.

1.35 The legislation prohibits the disclosure of information obtained through interception except in defined circumstances, including in the course of giving evidence in proceedings provided the information is admissible in accordance with another provision of the legislation.

1.36 Written notification of an authorized interception is required to be given to the person who was the object of the interception within 90 days of the authorization or such further period not exceeding 3 years as is substituted by a judge.

1.37 The Solicitor-General must report annually to Parliament (and the Attorney-General of each province must publish a report) on the number of applications made for interception authorizations, the number granted and refused, the number of authorizations given in respect of each offence and certain other information. The latest available report (for the year 1985) records that all of the 504 applications made for non-emergency authorizations were granted.

The United Kingdom

1.38 *The Interception of Communications Act 1985* created for the first time in the U.K. a statutory framework for the authorization of interception of communications sent through the post or a public telecommunications system.

1.39 The expression 'interception' is not defined by the Act but the responsible Minister has stated that listening devices and other forms of surveillance are not covered.

1.40 The Act creates an offence of intentionally intercepting communications in the course of their passage through the post or a public telecommunication system. There are exceptions for interceptions:

a. under a warrant issued by the Secretary of State -

(1) in the interests of national security;

(2) for the purpose of preventing or detecting serious crime, ie, involving violence, resulting in substantial gain or conducted by a large number of persons in pursuit of a common purpose, or where it could reasonably be expected that a person with no previous convictions would be sentenced to imprisonment for three years or more.

(3) for the purpose of safeguarding the economic well-being of the United Kingdom (in this case only where the information which it is considered necessary to acquire is information relating to the acts or intentions of persons outside the United Kingdom).

b. made with the consent of the sender or recipient;

c. made in connection with the provision of postal or telecommunications services, or

d. in the case of communications transmitted by wireless telegraphy, made with the authority of the Secretary of State for purposes in connection with the issue of wireless telegraphy licences or the prevention or detection of interference with wireless telegraphy.

1.41 A warrant will normally be valid for a period of 2 months from the date of issue though a renewal is available which in the case of warrants for national security and economic purposes can be for a further period of 6 months.

1.42 The Act also:

a. requires the making of arrangements to safeguard intercepted material and to limit the use made of it;

b. prohibits, subject to certain exceptions (including prosecutions for illegal interception), the adduction in court of tribunal proceedings of evidence, and the asking of questions in cross-examination, tending to suggest that a Crown servant has illegally intercepted a communication covered by the Act, or that a warrant has been issued to such a servant, and

c. establishes a Tribunal to investigate applications by any person who believes that communications sent to or by him have been intercepted. In the case of warranted interceptions, the Tribunal is to determine whether the Act's requirements have been met. Where it finds that those requirements have not been met, the Tribunal may quash the relevant warrant, direct the destruction of copies of the intercepted material, and/or direct the payment of compensation to the applicant.

The United States of America

1.43 Title III of the Federal Omnibus Crime Control and Safe Streets Act of 1968 (Sections 2510 to 2520 of title 18, US Code) regulates the electronic and mechanical interception of wire and oral communications and the disclosure of intercepted information. (Only conversations that are capable of being heard by the human ear are covered; data transmission, the video part of videotaping and other forms of visual surveillance and monitoring devices are not.) Such interception is prohibited except for:

a. interception by law enforcement officials under a court order;

b. certain telephone company monitoring to ensure adequate services or to protect company property;

c. surveillance of a conversation where one participant consents to the surveillance, and

d. surveillance for national security purposes which is covered by the Foreign Intelligence Surveillance Act of 1978.

1.44 Applications for an order from a federal judge must be authorised by the US Attorney-General or a specially designated Assistant Attorney-General. The application must include details of the crime or crimes under investigation, the nature and location of the facilities or places to be monitored, the types of communication sought, and details of previous applications involving any of the same persons, facilities or places. The application must also state the identity, if known, of the person whose communications are to be intercepted.

1.45 A court must make four findings before warranting interception by law enforcement officials:

a. that probable cause exists to believe an individual has committed, is committing, or is about to commit one of the crimes specified in the statute (these include any offences punishable by death, espionage, treason, murder, kidnapping, extortion, bribery, gambling, embezzlement, counterfeiting and drug offences).

b. that probable cause exists to believe incriminating communications will be intercepted;

c. that less intrusive investigative techniques have failed, probably would fail, or are too dangerous, and

d. that probable cause exists to believe the place or facilities to be monitored are being used or will be used in connection with the commission of a crime or are leased to, listed in the name of, or commonly used by the suspect.

1.46 A court order may not authorize surveillance for more than 30 days although extensions may be granted. A court may require progress reports to facilitate supervision of the surveillance and the judge who issues the order must receive the recordings of intercepted communication immediately after the surveillance period specified has expired. The court must seal the application for the order, the order itself and all recordings made pursuant to it. (The statute provides that courts may admit intercepted communications in a criminal proceeding only when the communications are sealed properly or when the Government explains adequately the absence of a seal).

1.47 No later than 90 days after termination of the surveillance period, notice of the surveillance must be given to those persons named in the surveillance order and, as the judge requires, to other persons whose conversations have been intercepted, unless the judge agrees to postpone the notice. An individual who is named in the order or application or who is a party to an intercepted communication has a limited right to inspect the court order, application, and intercepted communications. The Government cannot use the contents of an intercepted communication as evidence, or otherwise disclose it in any trial, or other proceeding, unless each party is provided with a copy of the application and court order at least 10 days before the proceeding.

1.48 Violations of the statute may trigger judicial sanctions, including suppression of evidence, citations for contempt of court, civil damages, and criminal sanctions. The statute prohibits the manufacture, distribution, possession, and advertising of devices for electronic surveillance for non-public use.

1.49 Provision is made for interception by State authorities if a State passes legislation modelled on the Federal statute for the investigation of specified offences. (As at 31 December 1984, some 29 States and the District of Columbia had authorized their law enforcement officials to intercept.)

1.50 The April 1985 report by the Administrative Office of the U.S. Courts indicates that in 1984, federal and state judges approved 801 out of 802 requests for electronic surveillance - 289 by federal judges and 512 by state judges. The 1984 combined total was the highest since 1973. Equivalent figures for 1985 show that there were 786 requests for electronic surveillance, with 784 approvals, 243 by federal judges and 541 by state judges.

1.51 Amendments to the 1968 Act are proposed in the Electronic Communications Privacy Act 1986, a Bill for which is now before the U.S. Congress. The Act provides procedures by which law enforcment agencies may obtain access to both electronic communications (with some exceptions, eg the radio portion of a cordless telephone communication) and the records of an electronic communications system. The Bill continues to distinguish between wire or oral communications (voice) and electronic communications (data and video) for the purpose of some of the procedural restrictions currently contained in the 1968 Act. For example, court authorization for the interception of a wire or oral communication may only be issued to investigate certain crimes specified in the 1968 Act. An interception of electronic communication pursuant to a court order may be utilized during the investigation of any federal felony.

1.52 The US Congress is presently wrestling with the same moral and philosophical problems which have confronted this Committee during the course of its inquiry. It is worth re-stating here the fundamental principles discerned by the Chairman of the US House of Representatives Judiciary Committee when he presented his Committee's report and Bill to the House:

> The first principle is that legislation which protects electronic communications from interceptions by either private parties or the Government should be comprehensive, and not limited to particular types or techniques of communicating. For example, it is technically impossible to effectively differentiate between wire line phone calls and those which are carried by wire, microwave, satellite, and radio. Any attempt to write a law which tries to protect only those technologies which exist in the marketplace today, that is, cellular phones and electronic mail, is destined to be outmoded within a few years.
>
> The second principle which should be followed in this area is a recognition that what is being protected is the sanctity and privacy of the communication. We should not attempt to discriminate for or against certain methods of communication, unless there is a compelling case that all parties to the communication want the message accessible to the public.
>
> The third principle we should keep in mind is that the nature of modern recordkeeping requires that some level of privacy protection be extended to records about us which are stored outside the home ... Many Americans are now using computer services, which store their bank records, credit card data, electronic mail and other personal data. If we fail to afford protection against governmental snooping in these files, our right of privacy will evaporate.
>
> Today Congress stands at a cross-roads with respect to electronic communications privacy. We may provide the forum to balance the privacy rights of citizens with the legitimate law enforcement needs of the Govenment; or we abdicate that role to ad

hoc decisions made by the courts and the executive branch. I believe this bill is a significant step in that direction, and I urge my colleagues in the House to support this landmark legislation.[13]

Sweden

1.53 Mr Justice Stewart observed in his Report that the Swedish Constitution declares illegal any form of telephone interception except as expressly provided by law. As outlined in Section 16 of Chapter 27 of the Swedish Code of Judicial Procedure, Swedish law presently provides as follows:

> If a person reasonably can be suspected of an offence punishable by imprisonment for at least two years, and it is found of extraordinary importance for the investigation that the investigating authority or the prosecutor obtains knowledge of conversation to and from the suspect's telephone or any other telephone that can be assumed to be used by him, the court may authorize wire-tapping of the conversations. The question of such authorization may be considered by the court only on request of the investigating authority or the prosecutor.
>
> Authority for a wire-tap shall contain a time limitation, not to exceed one week from service of the authorization upon the manager of the telephone office. If, however, the suspicion relates to a grave drug offence or to grave smuggling of drugs pursuant to section 1 of the Ordinance relating to Narcotic Drugs (1962:704), wire-tapping may be authorized for at most one month from the said date.
>
> As to inspection of the records of a wire-tap, the provisions in section 12, first paragraph, on examination and inspection of private documents shall correspondingly apply. To the extent that the record contains matters of no importance for the investigation, it shall be destroyed immediately after inspection.[14]

Endnotes

1. H.R. Deb. (1.5.86) 2882.

2. H.R. Deb. (4.6.86) 4596.

3. This reference, and the earlier selections from the Letters Patent, were drawn from Appendix A(i), Report - Volume One, Royal Commission of Inquiry into Alleged Telephone Interceptions, the Hon. Mr Justice D.G. Stewart, 30 April 1986, pp361-365 (henceforth cited as 'Stewart, Report').

4. Stewart, Report, pp354-356.

5. Evidence, p85.

6. Evidence, p354.

7. Evidence, p327.

8. Evidence, p56.

9. Stewart, Report, pp304-307.

10. Stewart, Report, pp304-305.(The AFP gave an indication of the rejection rate of the Special Projects Committee - in the 3 weeks immediately preceding, the Committee had rejected 4 of 6 applications outright, in the main because of incomplete documentation: Evidence, p145)

11. Evidence, pp65-66.

12. Letter and attachments sent to the Committee Secretary by the Attorney-General's Department and dated 23 October 1986 (paragraphs 1.29 - 1.51 are adapted from one of the papers attached to this letter entitled 'Telecommunications Interception - Overseas Legislation') - Exhibit 26.

13. US Congressional Record - House, 23 June 1986, ppH4046 - H4047.

14. The Swedish Code of Judicial Procedure, the National Council for Crime Prevention, Report No 16, Stockholm, May 1985, p102.

AUSTRALIAN FEDERAL POLICE

TELECOMMUNICATIONS INTERCEPTION POLICY

CONTENTS

INTRODUCTION

1. Definition: This document defines the policy to be followed by members of the AFP in respect of action taken under or proposed pursuant to the provisions of the Telecommunications (Interception) Act 1979, (hereinafter referred to as 'the Act').

Members are to be aware that the provisions of the Act relate directly to the right to privacy of the individual and I require that the legislation be strictly complied with to provide the highest standards of accountability. No departure from the legislation will be permitted.

Questions of interpretation of the Act are to be referred to the Assistant Commissioner Investigations for resolution prior to any action being taken.

2. Description: This policy determines responsibilities for action required by members of the AFP and describes the administrative procedures to be followed in telecommunications and telegram interception and handling of the resultant product.

3. Purpose: The purpose of the interception of telecommunications and telegrams by members of the AFP is to assist in the collection of information in respect to AFP inquiries into narcotics offences as defined by the Act. Telecommunications or telegram interception may be instituted only in respect of AFP inquiries into 'narcotics offences' as defined under the Act.

4. Security: The highest degree of security, consistent with practicalities, is to be afforded to all aspects of telecommunications interception by members of the AFP. The words 'Telecommunications Interception', 'Telephone Interception'

.../2

or 'Telegram Interception' are not to be used in unclassified documentation or over unsecured telecommunications lines. The general term 'Special Projects' should be used whenever possible in connection with AFP telecommunications interception activities.

5. Policy Limitations: This policy directive defines the AFP policy in respect of telephone and telegram interception only. Consideration of interception of telecommunications other than telephone and telegram is to be referred to the Assistant Commissioner Investigations Department prior to any intercept action taking place.

6. Listening Devices: This policy document relates solely to telecommunications interception. A separate policy document will be issued in respect to listening devices.

7. Command and Control: The Assistant Commissioner Investigations Department is responsible, subject to the statutory obligations imposed on me as Commissioner of Police, for exercising control over all AFP telecommunications interception.

TELEPHONE INTERCEPTION

8. Special Projects Branch: The Commander Special Projects Branch is responsible through the chain of command to ensure compliance with the administrative provisions of the Act: for providing telephone interception services; documentary and tape controls in respect of the service; management of the interception service; arrangements for approval to seek issue of warrants; and liaison with staff of the Australian Telecommunications Commission.

.../3

9. Electronic Services Branch: The Commander Electronic Services Branch of the Logistic Services Division is responsible for providing the necessary equipment, services and maintenance to the Special Projects Branch to execute the telephone interception services.

10. Intelligence Division: In accordance with the provisions of paragraph 13 of this policy the Commander Intelligence Division is responsible for coordinating the distribution and dissemination of information obtained from a telecommunications interception and communicated in accorance with the Act.

11. Special Projects Committee:

(1) A Special Projects Committee chaired by the Assistant Commissioner Investigations Department and comprised of Divisional Commanders, Investigations Department will be responsible for consideration of applications for approval to seek the issue of special projects warrants and determination of priorities for special projects.

(a) Three members of the Special Projects Committee will constitute a quorum.

(b) The Commander Special Projects Branch is both Secretary and a member of the Special Projects Committee.

(2) The Special Projects Committee will consider all applications for telecommunications interception warrants as soon as practicable after receipt by the Commander Special Projects Branch. The Commander

.../4

Special Projects Branch will examine all applications and seek clarification or further information as necessary, before putting the application before the Special Projects Committee.

(3) When an application from a Region is approved, the Commander Intelligence Division will, if considered necessary by the Committee, require the Commander B.C.I. to appoint a B.C.I. 'Case Officer' to maintain an overview of the interception in consultation with the R.I.U. 'Case Officer'.

12. (1) Applications for Warrants: An application for an interception warrant is to consist of:

(a) a recommendation under the personal signature of the Regional Commander. This recommendation is also to address the availability of staff resources to act on information received. This provision also applies to applications from members attached to Joint Task Forces working in a Region of the A.F.P.;

(b) an explanatory brief signed by a Commissioned Officer or member acting as a Commissioned Officer setting out the complete background of the application;

(c) a draft affidavit, in the name of a member at no less than the substantive rank of Station Sergeant, which may include information in regard to more than one telecommunications service, provided the information concerning each service is the same and the telecommunications services are in the same State;

.../5

(d) a draft warrant for each telecommunications service involved.

(e) an order of priority where there is more than one application for the same operation/information.

(2) Applications for telecommunications interception warrants shall:

(a) be forwarded under confidential cover to the Commander Special Projects Branch;

(b) prior to forwarding shall be checked for accuracy and consistency. No abbreviations or colloquialism shall be used, unless the latter is in quotation;

(c) be prepared where practicable by a Case Officer in the Regional Intelligence Unit (RIU). Where applicable the RIU Case Officer will consult with the relevant Operational Unit Case Officer;

(d) when an application originates in a Headquarters Unit, be prepared by a Case Officer in the Bureau of Criminal Intelligence (BCI) Headquarters. Where applicable, the BCI HQ Case Officer will consult with the relevant Operational Unit Case Officer. The application is to be forwarded to the Commander Special Projects Branch under the signature of and with a recommendation by the Commander Intelligence Division; and

.../6

(3) Upon approval of an application by the Special Projects Committee, The Commander Special Projects Branch will cause the necessary administrative arrangments to be made to obtain and execute the warrant.

13. (1) Information Dissemination:

(a) information from an intercept will be communicated, strictly in accordance with sub-sections 7(4) and 7(5) of the Act. Communication pursuant to sub-section 7(4) of the Act will be from Special Projects Branch staff to BCI members designated for that purpose. Where an operational urgency exists information to be communicated pursuant to sub-section 7(4) of the Act may be released by Special Projects Branch staff direct to RIU or Operational Unit Case Officers in the absence of the BCI members. It is to be noted that communication of information pursuant to sub-section 7(5) of the Act is governed by section 19 of this policy;

(b) Those BCI members will be responsible, under the direction of the Commander Special Projects Branch, for the timely distribution of the information to the relevant RIU or JTF Case Officer and/or BCI HQ Case Officer;

(c) Those same BCI members will maintain liaison with and between RIU Case Officers the Operational Unit Case Officer and Special Projects Branch staff; and

.../7

(d) The RIU or BCI Case Officer will be responsible for processing the information provided and for timely dissemination of intelligence to the Operational Unit Case Officer.

(2) Notwithstanding the provisions of sub-paragraphs (b)(c) or (d) of sub-section (1) above, in those Regions in which a member has been designated a 'Special Projects' member by the Assistant Commissioner Investigations Department, the BCI members mentioned in sub-paragraph 13(1)(a) shall distribute the information directly to that designated 'Special Projects' member.

14 (1) Effectiveness Reporting

(a) Responsibility: Regional Commanders will be responsible for ensuring effectiveness reports are submitted on all telecommunications interception warrants issued in their Region (including those relevant to Joint Task Forces).

(b) Divisional Commanders Investigations Department Canberra will be responsible for ensuring submission of effectiveness reports in respect of warrants issued on application from members in their Division.

(c) Effectiveness reports shall be submitted under confidential cover so as to reach the Commander Intelligence Division no later than the close of business on the second Monday of every month.

.../8

(d) On the second Tuesday of every month the Commander Intelligence Division shall provide a copy of each effectiveness report received for that month to the Commander Special Projects Branch.

(2) Effectiveness Reports shall:

(a) advise the use made by members of information obtained by intercepting communications or inspecting telegrams, as the case may be;

(b) advise whether the facts and other grounds on which the warrant was issued, still apply. If not, what variations now apply or exist;

(c) advise the location and storage arrangements of transcripts/ recordings containing the information received; and

(d) indicate if any of the information received has been communicated to persons other than members of the A.F.P.

15. Status Reporting: Each 60 days from the date of commencement of operation of this Policy, the Commander Special Projects Branch through the normal chain of command is to furnish the Assistant Commissioner Investigations Department, with a Status Report of telephone interceptions.

16. Destruction or Retention Recommendations:

(1) Within 30 days of the cessation of an interception, the appropriate Regional or Divisional Commander is to provide the Commander Special

.../9

Projects Branch with a recommendation that the records of the intercepted communications be destroyed or not, in accordance with Section 24 of the Act. The Commander Special Projects Branch will process such recommendation for final decision and authorisation by the Commissioner.

(b) The Commander Special Projects Branch will be responsible for the destruction or secure retention of the records as directed by the Commissioner.

(c) Where retention of records has been recommended the Regional or Divisional Commander shall cause a review of this recommendation each six months thereafter and shall advise the Commander, Special Projects Branch of the outcome of this review.

17. Evidentiary Usage: Information from telecommunications interception may be given in evidence in a proceeding by way of a prosecution for an offence as provided for by sub-section 7(6) of the Act. All requests to use such information as evidence are to be forwarded to the Assistant Commissioner Investigations Department by the appropriate Regional Commander or the Commander Intelligence Division.

18. Investigation Usage: The use of taped conversations communicated pursuant to the Act and extracted from information obtained in accordance with the provisions of the Act, is permitted in interviews of persons suspected of involvement in narcotics offences. Permission to use the information in this manner must be obtained from the Assistant Commissioner Investigations.

.../10

19. The communication of information pursuant to sub-paragraph 7(5) of the Act, where such information is obtained by -

(1) virtue of a warrant issued under section 20 of the Act, may -

(a) in respect to matters appearing to involve the corruption of public officials, be made by the Commissioner. The Commander Special Projects Branch shall bring all such instances to the Commissioner's attention; and

(b) in respect to matters appearing to implicate police in criminal activities, be made by the Commissioner. The Commander Special Projects Branch shall bring all such instances to the Commissioner's attention; and

(2) virtue of a warrant issued under section 21 of the Act, shall be made by the Commissioner.

TELEGRAM INTERCEPTION

OVERVIEW

20. It is recognised that the circumstances in which members of the AFP may require a warrant for interception of a telegram may differ to those pertaining to telephone interception in terms of time frame and location.

RESPONSIBILITIES

21. Where relevant and applicable the responsibilities outlined in paragraphs 8, 10 and 11 apply in respect to telegram interception.

.../11

INTERCEPTION

22. The procedures outlined in paragraphs 12, 13, 14, 15, and 16 are to apply in respect of telegram interceptions.

23. Warrant: Upon approval of an application by the Commissioner, the Commander Special Projects Branch will undertake the necessary administrative arrangements to obtain the warrant. In conjunction, the Commander Special Projects Branch and the Commander BCI will arrange for the execution of the warrant.

24. Dissemination: The Commander Intelligence Division shall determine the dissemination of the copies of the telegrams in accordance with the provisions of the Act.

It is unlawful for a member of AFP acting in his capacity as such to seek from the Australian Telecommunications Commission, or from an officer of that Commission, access to a telegram or information concerning the contents of a telegram except in pursuance of, or for the purposes of, a warrant under the Act. All members are to be aware of this provision of the Act and are to ensure that it is not contravened.

REVOCATION OF WARRANTS

25. (1) Where, before a warrant issued under section 20 or 21 of the Act, ceases to be in force, the grounds on which the warrant was issued appear to have ceased to exist the appropriate Regional or Divisional Commander shall notify the Commander Special Projects Branch by the most expeditious means available of the changed circumstances.

...12

(2) The Commander, Special Projects Branch shall ensure that the interception of communications or the inspection of telegrams, as the case may be, ceases forthwith pending a decision by the Commissioner as to whether or not the relevant warrant is to now be revoked.

(3) The Commander Special Projects Branch shall submit suitable documentation and recommendation to the Commissioner concerning revocation of the relevant warrant as soon as possible in each such instance.

CONCLUSION

26. All members must be cognizant of the considerable responsibilities incumbent on the AFP in respect of telecommunications interception powers. The Act's provisions should not be used where normal policing methods and good investigative practices will suffice.

26. This Policy is effective immediately.

2 August 1985

(R. A. Grey)
Commissioner of Police

CHAPTER 2

THE 1986 BILL

Introduction

2.1 In his second reading speech on 4 June 1986, the Attorney-General stated that:

> The new provisions (in this Bill) will provide Australian law enforcement authorities with an important additional tool in the investigation and prosecution of serious drug trafficking offences, while at the same time providing effective safeguards for the protection of personal privacy.[1]

2.2 With a focus on the Attorney-General's objectives, this Chapter will describe firstly how the Bill alters the Act.[2] This will be achieved by examining the three major proposals which are:

a. to extend the existing telecommunications interception powers of the Australian Federal Police (AFP) which currently only apply to certain Commonwealth narcotics offences punishable under the Customs Act to a wider category of serious drug trafficking offences. These are defined as those offences against Commonwealth laws involving narcotic drugs and attract punishment by imprisonment for life or for a maximum period of 7 years or any period between 7 years and life imprisonment;

b. to make available interception powers in respect of serious drug trafficking offences to the National Crime Authority (NCA), and

c. to make available interception powers in relation to serious trafficking offences against State and Territory laws to State and Territory police forces.

2.3 Secondly, this Chapter will examine the reactions to the legislation, as revealed in submissions to the Committee and evidence taken during the course of its inquiry.

2.4 The Bill proposes a number of changes relating to the use and communication of intercepted information which are provided for under section 7 of the Act. Fundamental to the scheme of the Act is sub-section 7(1) which provides:

> 7 (1) A person shall not -
>
> (a) intercept;
>
> (b) authorise, suffer or permit another person to intercept; or
>
> (c) do any act or thing that will enable him or another person to intercept,
>
> a communication passing over a telecommunications system. Penalty: $5000 or imprisonment for 2 years.

This provision of course does not apply to the interception of a communication in pursuance of a warrant (paragraph 7(2)(b)). Currently the use in evidence of information obtained from intercepted communications is facilitated by sub-section 7(6) of the Act. The provisions are that:

> Without limiting the application of sub-section (4) a person may give information obtained by intercepting a communication passing over a telecommunications system, or obtained by virtue of a warrant issued under section 11 or 21, in evidence in a proceeding -
>
> (a) by way of a prosecution for a narcotics offence;

(b) by way of a prosecution for an offence against the Telecommunications Act 1975 or a regulation in force under that Act;

(c) by way of a prosecution for any other offence against the law of the Commonwealth or of a State or Territory punishable by imprisonment for life or for a period or maximum period, of not less than 3 years;

(d) by way of an application for an order under sub-section 243B(1) of the Customs Act 1901; or

(e) for the condemnation or recovery of a ship or aircraft or of goods, seized under section 203 of the Customs Act 1901 in connection with the commission of a narcotics offence.

Sub-section 7(4) which is referred to in the opening words of sub-section 7(6) prohibits the communication to any other person or the use or recording of information obtained by the interception of a communication passing over a telecommunications system or obtained by virtue of a warrant except in certain specified circumstances which are not material for present purposes. It is evident that the provisions of sub-section 7(6) allow the use of information obtained pursuant to a warrant in proceedings relating to a wide range of Commonwealth and State offences and not limited to narcotics offences.

2.5 In summary, therefore, the Bill amends section 7 and includes new provisions dealing separately with the prohibition of unauthorised interceptions, the regulation of the use and communication of intercepted information and the admissibility of such information in evidence in proceedings. Information obtained in contravention of the Act would be inadmissible in evidence in any court except for the purpose of establishing the contravention of the Act. In his second reading speech, the Attorney-General summarised the most important effects of the new provisions. They are as follows:

a. it would continue to be an offence to intercept communications passing over a telecommunications system except pursuant to a warrant or as otherwise authorised by the Act;

b. it would be an offence to use, record or communicate to a person or a court or tribunal material obtained in contravention of the Act, except for the purpose of establishing that contravention;

c. it would be an offence to use, record or communicate to a person or a court or tribunal material that has been lawfully obtained, except in accordance with the Act;

d. communication of lawfully obtained material would be permitted between the Australian Federal Police, State and Territory police forces, the National Crime Authority and the State Drug Crime Commission and the Australian Security Intelligence Organisation, where the material is relevant to their functions;

e. it would be possible to give lawfully obtained information in evidence only in the proceedings specified in draft section 7AB. Information obtained in contravention of the Act will be inadmissible in all proceedings except to establish the contravention. This exclusionary rule is, however, subject to a discretion in the court to admit information where the contravention is due to an insubstantial defect or error in cases where a warrant has been obtained.[3]

2.6 On 11 June 1986 after consideration of the Bill the Senate Standing Committee for the Scrutiny of Bills reported that:

> New sub-section 7AB(7) would permit the Attorney-General to waive non-compliance with the procedures for the granting of a warrant at the request of the Director-General of Security and to approve

the admission of evidence obtained by the interception of telecommunications purportedly in compliance with a warrant granted under section 11A but in fact in contravention of the prohibition in sub-section 7(1) of the Act. The provision contrasts with the power to waive similar non-compliance in the grant of warrants to the Australian Federal Police in new sub-section 7AB(3) in that this latter power is conferred on the courts and restricted to the waiver of insubstantial defects or irregularities.

As the power to grant warrants under section 11A is vested in the Attorney-General it appears that the Attorney-General might be waiving his own non-compliance with the provisions of that section. Moreover the failure to restrict the ambit of the waiver to insubstantial defects or irregularities would appear to have the effect that, even if the Attorney-General could not have been satisfied at the time of granting the warrant that the collection of intelligence relating to a particular matter was important in relation to the defence of the Commonwealth or to the conduct of the Commonwealth's international affairs (the test set out in paragraph 11A(1)(b)), the Attorney-General may nevertheless approve the admission in evidence of information obtained in purported reliance on the relevant warrant.

The Committee therefore draws the new sub-section to the attention of Senators in that, by permitting the requirements for the grant of a warrant in section 11A to be evaded, it may be considered to trespass unduly on personal rights and liberties.[4]

2.7 Subsequent to this finding the Attorney-General's Department advised the Committee that the Attorney-General had decided to delete sub-section 7AB(7) from the Bill.[5]

2.8 Under the existing statutory framework, section 20 of the Act empowers Judges of the Federal Court to issue warrants authorising the interception by officers of the AFP of

communications made to or from the telecommunications service. The power conferred by section 20 on Federal Court Judges may also be exercised by Judges of the Supreme Courts of a State or Territory in respect of whom an appropriate intergovernmental arrangement is in force under section 19 of the Act. In this part of the Act 'Judge' is defined as follows:

a. a Judge of the Federal Court of Australia or of the Supreme Court of the Australian Capital Territory;

b. a Judge of the Supreme Court of a State in respect of whom an appropriate arrangement in force under section 19 is applicable; or

c. a Judge of the Supreme Court of the Northern Territory who is not a Judge referred to in paragraph (a) and in respect of whom as appropriate arrangement in force under section 19 of this Act is applicable.

The Extension of the AFP's Existing Telecommunications Powers

2.9 Sections 20 and 21 of the Act would be amended to extend the present powers of the AFP in relation to telecommunications interception and telegrams inspections. Presently the powers only relate to 'narcotics offences', but will be extended to cover also 'serious drug trafficking offences' which are defined as narcotics offences and any other Commonwealth or Australian Capital Territory offences involving narcotic drugs that are punishable by imprisonment for life, or for a maximum period of not less than seven years or longer. Further, there would be a new requirement that a Judge, in deciding whether or not to issue a warrant for either telecommunications interception or inspections of telegrams, must be satisfied that the information sought is not readily available

from another source. Further, the Judge must be satisfied that there are reasonable grounds for suspecting that the telecommunications service is being or is likely to be used by a person who has committed, or is suspected on reasonable grounds of having committed, or of being likely to commit, a narcotics offence, and that the interception by members of the AFP of communications will, or is likely to, assist them in connection with enquiries being made in relation to the commission or likely commission of a narcotics offence. At the same time the Judge would be required to take care not to prejudice the investigation if the warrant is not approved. (Clauses 9 and 10)

2.10 Further, amendments proposed to section 20 would enable a Judge to issue a warrant upon an application made by telephone, by specially authorised members of the AFP, in circumstances of urgency. (Proposed sub-sections 20(3A), (3B), (3C), (3D), and (3E)

2.11 In relation to the interception of telecommunications and the inspection of telegrams, the maximum period for which a warrant may remain in force would be reduced from 6 months to 90 days. (sub-section 20(5))

2.12 Section 23 of the Act details two functions relating solely to the Commissioner; to discontinue an interception and revoke the warrant in writing after the warrant ceases to exist. It is proposed in the Bill to extend the legal right to effect these functions to the Deputy Commissioner.

2.13 By virtue of Clause 12 of the Bill the duty to destroy irrelevant records would rest with the authority that has possession, custody or control of the records. (section 24)

2.14 The existing penalty of a fine of $1,000 for obstructing or hindering a person acting in pursuance of a warrant under section 20 or 21 would also include imprisonment for 6 months. (section 26)

2.15 Clause 16 proposes to insert new section 27A, requiring the Minister [Attorney-General] to report annually to the Parliament on the number of warrants issued to the AFP during the preceding year and the use made of information obtained by virtue of those warrants. The report, however, must be in terms that do not enable the identification of any person.

The Availability of Interception Powers to the NCA

2.16 The Bill proposes that the NCA be given telecommunications interception powers in relation to any such offences that are under the subject of an investigation by the NCA under its Act. This would be done by the insertion of a new Part VI (Clause 61). Although the interception powers proposed for the NCA are similar in many respects to the AFP they differ in two main aspects. The NCA would not be given the power to intercept in their own right, rather, they would be required to facilitate the interceptions through Telecom. Secondly, a warrant issued to the NCA would not authorise any entry upon premises.

2.17 As with the AFP, proposed section 33 provides that judicial warrants will be available to the NCA in relation to *serious trafficking offences where the offence is the subject of* an investigation by the NCA. In Part VI, 'Judge' is defined as for the definition applying to 'Judge' in relation to Part IV. The Judge must be satisfied, on the basis of information furnished to the Judge that:

a. the Authority is conducting a prescribed investigation under its Act in relation to a serious trafficking offence;

b. there are reasonable grounds for suspecting that the relevant telecommunications service is being, or is likely to be, used by a person who is

committing or has committed, or who is suspected on reasonable grounds of committing or having committed, that offence;

c. the interception of communications to or from the service will, or is likely to, assist the Authority in the investigation, and

d. the information sought is not readily available from another source, having regard to any prejudice to an inquiry likely to result from a refusal to grant an interception warrant.

2.18 Applications would normally be required in writing supported by information on oath. In cases of urgency, however, a warrant could be issued on an application made by telephone. (Proposed sub-sections 33(2), 33(4), 33(5), 33(6) and 33(7).

2.19 As with the AFP, proposed sub-section 33(10) deems that a warrant sought by the NCA would remain in force for a maximum period of 90 days, and would authorise approved persons to intercept, that is listen to, or record, communications passing over the service specified in the warrant. (Proposed section 34)

2.20 Proposed sub-section 33(8) provides that the warrant would not authorise any entry upon premises and would require that all interceptions be conducted through Telecom.

2.21 Proposed section 35 would require that, when the NCA Chairman is satisfied that the grounds upon which a warrant was issued have ceased to exist, the Chairman would be required to revoke the warrant and take immediate steps to ensure that interceptions pursuant to the warrant are discontinued.

2.22 The Chairman is also required to ensure the destruction of all records or copies of intercepted communications in the possession, custody or control of the NCA if the records are not needed for the purposes of lawful use or communication by the NCA. (Proposed section 36)

2.23 The NCA would be required to inform the Managing Director of Telecom of the issue and revocation of each warrant and to provide the Director with a certified copy of each warrant and instrument of revocation. It would be required to retain in its own records copies of all warrants and instruments of revocation. (Proposed section 37)

2.24 Proposed section 38 would make it an offence to obstruct or hinder, without reasonable excuse, a person acting pursuant to a warrant.

2.25 The Chairman would be required to send to the Attorney-General reports on the issue and revocation of each warrant and on the use and communication of information obtained pursuant to warrants. (Proposed section 39)

2.26 The Attorney-General would be required to report to the Parliament annually on the number of warrants issued during the preceding year and, in terms that do not enable the identity of any person to be disclosed, the use made of information obtained pursuant to those warrants. (Proposed section 40)

The Extension of Interception Powers to State and Territory Police Forces

2.27 The aim of Part VII, which would be an addition to the Act, is, according to the Attorney-General, to:

> impose direct responsibility on State and Territory authorities and Ministers for the proper conduct and oversight of intercept

activities, while at the same time ensuring that the Commonwealth Government is able to discharge its overall responsibilities in this area.[6]

2.28 In Part VII 'eligible Judge', in relation to a State, means a person who:

a. except where paragraph (b) applies - is a Judge of the Supreme Court of that State; or

b. in the case of the Northern Territory - is a Judge of the Supreme Court of that Territory and is neither a Judge of the Federal Court of Australia nor a Judge of the Supreme Court of the Australian Captial Territory, and

who is designated, or is included in a class of persons that is designated, by or under the law of the first-mentioned State, to perform the functions under this Part of an eligible Judge of the first-mentioned State.

2.29 The provisions contained in Part VII would not only extend telecommunications interception powers to the State and Territory police forces, but also to the State Drug Crime Commission of New South Wales. The Commission is subject to the same conditions and legislative safeguards that apply to the State and Territory police forces.

2.30 Fundamental to Part VII, (proposed section 43), is that interception powers in relation to serious drug trafficking offences against State and Territory laws would only be made available to those agencies declared, by notice in the Gazette, to be eligible authorities by the Attorney-General.

2.31 Proposed sub-section 43(3) would require the Attorney-General to be satisfied that the relevant State or Territory has entered into an agreement to pay all expenses incurred in connection with the issuing of warrants and the interception of communications for that authority, before making a declaration. Further, the relevant authority must have agreed to reimburse Telecom for all expenses incurred by Telecom in connection with those warrants.

2.32 A declaration would be made only at the request of the relevant Premier or Chief Minister and if the Attorney-General is satisfied that the applicable State or Territory has legislation that provides satisfactory safeguards (proposed sub-section 43(2)). Also contained in proposed sub-section 43(2) is a list of safeguards (said to be at least as stringent as those applying in relation to interceptions carried out by the AFP). These include:

a. provisions for reporting on the issue and revocation of warrants to the relevant State or Territory Minister;

b. proper maintenance of records by the State or Territory police force;

c. regular inspection of those records by an independent authority;

d. reporting by that authority on the extent of compliance with statutory requirements;

e. destruction of irrelevant records, and

f. regular reporting by the relevant State or Territory Minister to the Commonwealth Minister.[7]

2.33 Proposed sub-section 43(4) would empower the Attorney-General to revoke a declaration where the relevant State or Territory law is not maintained, where compliance with the law is unsatisfactory, where the agreement in relation to the payment of expenses has ceased or is unsatisfactory, or where there is not satisfactory compliance with the provisions of the principal Act. A declaration may also be revoked on request by the relevant Premier or Chief Minister. As the Attorney-General told the House:

> By means of these provisions, the Commonwealth will be able to ensure, as far as possible, that there is a continuous monitoring and control at the State or Territory level of day to day activities by State or Territory officers. The issue and revocation of warrants, the scope of the authority conferred by warrants, and the communication of information will be controlled directly by the provisions of the Telecommunications (Interception) Act.[8]

2.34 Under proposed section 44, warrants would be issued by State Supreme Court Judges, on application by a relevant declared State or Territory Authority, in relation to serious drug trafficking offences against the laws of the relevant State or Territory. Proposed sub-section 44(4) would provide that telephone applications may be made by specially approved members of the State or Territory police force in circumstances of urgency. Normally applications would be in writing supported by information on oath (proposed sub-sections 44(2) and (3)).

2.35 A warrant would only authorise interceptions in relation to telecommunications equipment situated within the State concerned ie confined to equipment within State borders, and only by means of equipment approved under the State law required by proposed section 43 (proposed sub-section 44(1)).

2.36 Proposed sub-section 44(10) would allow a warrant to remain in force for a maximum period of 90 days, and authorise interceptions by persons approved pursuant to a law of the relevant State or Territory.

2.37 Warrants would not authorise entry on to premises (proposed paragraph 44(9)(a)). Further, proposed paragraph 44(9)(b) would require that the interception be carried out through Telecom.

2.38 Proposed section 45 contains provisions for the revocation of warrants and the discontinuance of interceptions, while proposed section 46 contains provisions relating to notifying this information to the Managing Director of Telecom.

2.39 Proposed section 49 contains annual report provisions similar to those applicable to the AFP and NCA. The Commonwealth Attorney-General would be required to report annually to the Parliament on the numbers of warrants issued in each State or Territory and on the use made of information obtained under warrant.

Reactions to the Legislation

2.40 Community reaction to the proposed legislation is summarised in the following paragraphs in accordance with the format of the proposed Bill.

Interpretation

2.41 The implications of the insertion in the Act of certain definitions, for example, 'prescribed offence' and 'serious trafficking offence' gave grounds for some concern in submissions to the Committee. A 'serious trafficking offence' is to be defined after the amendment in the following terms:

a. a narcotics offence; or

b. any other offence against a law of the Commonwealth, or an offence against a law of a State or Territory, being an offence -

(i) that relates to narcotic drugs; and

(ii) is punishable by imprisonment for life or for a period or maximum period of not less than 7 years.

2.42 According to the Law Council of Australia a problem of interpretation arises immediately from the criterion in paragraph (b) of the definition that the offence be one that 'relates to narcotic drugs'. The proponent of a broad power would argue that an offence 'relates to' narcotic drugs if in the circumstances of the particular case there is some connection with narcotic drugs. A narrower view would contend that the importation, possession, use, sale or other disposal of narcotic drugs must be an element of the legal definition of the offence before it can be said to be an offence that 'relates to' narcotic drugs.

2.43 The Council's proposition is that the definition of serious trafficking offence under the Act leaves the scope of the power to issue warrants in an undesirable state of uncertainty.[9]

2.44 In their examination of the term 'serious trafficking offence', the Law Council of Australia determined:

> There is an internal inconsistency in the definition of 'serious trafficking offence' and that arises from its application across the board to 'narcotics offences' which under the definition of that term include offences punishable by no more than two years imprisonment and a fine of $2,000.00.
>
> Some of the offences caught within the scope of the term 'narcotics offence' as defined in the Bill include simple possession of a

> prohibited import and failure to comply with the conditions of an import licence.
>
> Patently it includes offences which are not in the Council's view 'serious trafficking offences.'[10]

2.45 According to the Council the anomaly exists presumably because it is not desired to reduce the existing powers of the AFP in connection with the obtaining of search warrants. The Council argues that it is an unwarranted downgrading of the public interest in the preservation of individual privacy to allow its violation in connection with the investigation of offences that are relatively minor and include what would be seen as purely regulatory offences.[11]

2.46 The Law Council of Australia concluded that one way of dealing with this internal inconsistency is to apply the same 7 year limit to narcotics offences as applies to the class of *offences covered by paragraph (b)*. If that view is accepted then there need no longer be a separate category of narcotics offence because it would all fall within the broader description in the second limb in any event. The appropriate course would be to replace that term by the term 'serious narcotic offence' and to define it as follows:

> 'Serious narcotic offence' means any offence against the law of the Commonwealth or an offence against a law of a State or Territory being an offence: -
>
> a. that arises out of or in connection with the importation, exportation, possession, use, sale or other disposal or any unlawful dealing in narcotic drugs; and
>
> b. is punishable by imprisonment for life or for a period or maximum period of not less than 7 years.[12]

2.47 In summary, therefore, the Law Council of Australia recommended the following:

a. The definition of 'serious trafficking offence' should be clarified so as to make it clear whether the term 'offence ... that relates to narcotic drugs' extends only to offences whose legal definition embodies some use or dealing in narcotic drugs as an element or whether it extends to offences which as a matter of fact arise in connection with narcotic drugs.

b. The term 'serious trafficking offence' should be redefined so as to ensure that it strikes at offences of the appropriate level of seriousness which arise out of or in connection with unlawful use of dealing with narcotic drugs.

c. The separate reference to 'a narcotics offence' in paragraph (a) of the definition ought to be dropped.

d. The term 'serious trafficking offence' ought to be replaced by the term 'serious narcotic offence'.[13]

2.48 It has been suggested that some definitions proposed by the Bill are incompatible with the wording of similar State legislation. The New South Wales Police describe one example. In New South Wales legislation, the definition of 'serious [trafficking] offence' refers to 'penal servitude', rather than 'imprisonment', as defined in 'serious offence' by the Federal legislation. Similarly, as the Victorian Police pointed out, the Victorian Drugs, Poisons and Controlled Substances Act 1981, does not recognise the expression 'narcotic drug', therefore, there may be an incompatibility between Federal and State law.[14] A number of other definitions it was suggested were either too wide, for example 'prescribed offence', or unclear in their meaning, for example, 'serious trafficking offence'. Following along the lines of the Law Council of Australia, a witness from the New South Wales Labor Lawyers argued for the insertion of a definition for 'narcotic offence'[15].

Scope of the Legislation

2.49 In regard to the scope of the legislation a general view was that the Bill should not confine itself to offences relating to drugs and national security. This view is exemplified in the submission of the Australian Law Reform Commission (ALRC):

> a warrant to intercept communications passing over a telecommunications service should be available in relation to all 'serious offences' so defined. The present restriction to 'narcotics offences' and the restriction that would obtain upon the passage of the Bill to 'serious trafficking offences' cannot it is suggested, be logically sustained.[16]

2.50 Opposing this view a witness from the New South Wales Labor Lawyers stated that the legislation should be restricted to trafficking in serious narcotic substances, but excluding indian hemp.[17]

2.51 The Law Council of Australia submitted that:

> If the legislation is to be directed at the drug trade, it should not be limited to those offences which by accident of definition involve some dealing with a narcotic drug as an element of the offence. The power ought to be made available in such a way as to deal with the substantive mischief of the trade and that means striking not only at those offences which are central to the operations of the drug trade but also the support structure of extortion, intimidation, serious assault and homicide.[18]

2.52 The Australian Telecommunications Employees Association (A.T.E.A.) expressed concern over the ambiguity of the scope of the legislation. The A.T.E.A. believes that the legislation should state clearly what forms of telecommunications services can be intercepted. They said:

> The technology of telecommunications is changing rapidly and so too are the services offered over the telecommunications network. Some new services, such as mobile cellular radio telephones, would not require a hard wired tap. All that would be needed would be a device which scans the relevant part of the radio frequency. The ATEA therefore believes that, as a matter or principle, the services which can be intercepted should be detailed in any revised legislation. It should be clear and it should be widely known and understood by the Australian people whether the following forms of telecommunication services fall within the ambit of the legislation: Data services such as Datel and Austpac; facsimile; electronic mail services such as Telememo; voice mail; telex; Teletex services and cellular radio.[19]

2.53 This sentiment was supported by the NCA:

> the Authority's view at this stage that it ought to have the power to intercept other types of telecommunication messages as well as telephone conversations. There does not seem to be any difference in kind between these various types of messages, and indeed the argument could be put that were the power to intercept only telephone conversations to be granted to the Authority and other law enforcement agencies, those people of interest to the Authority and other agencies may be the more disposed to use facsimile devices and the like. Were a general power to intercept telecommunications messages to be granted, it should of course be on the same basis with respect to safeguards by way of judicial warrant etc. as is now the case with telephone interceptions.[20]

2.54 Advice received from the Attorney-General's Department supported the proposition that interception legislation extends to non-verbal communications, eg, facsimile and telex:

> This Department has consistently advised that 'communication passing over a Telecommunications system' is not limited to speech. Any communication, that is any

> transmission of information or of a signal comes within the meaning of 'communication'. Accordingly, non-verbal means of transmitting information over telecommunications systems operated by the Australian Telecommunications Commission are covered by the provisions relating to interception contained in the Act.[21]

2.55 Chapter 4 examines whether the scope of the legislation should be extended in accordance with Stewart's recommendation to extend interception powers to serious offences.

Serious Offences - The Mechanism for Legislation

2.56 The mechanism for legislation with respect to 'serious offences' was canvassed in a minor way in written evidence, but pursued at length in oral evidence. The Committee received a variety of suggestions as to possible ways of dealing with 'serious offences'. These included:

a. 'serious offences' being defined according to the number of years of maximum or minimum sentence that can be imposed under criminal statutes;

b. the applicable 'serious offences' being specified in a list which would form part of the Act;

c. judicial discretion to evaluate 'serious offences' having cognisance of certain things, and

d. defining 'serious offences' as all indictable offences, and not therefore including summary offences.

2.57 Once again, Chapter 4 examines in more detail the mechanism for legislating in respect to serious offences.

Evidentiary Certificates and Admissibility of Evidence

2.58 In evidence, the Committee received widespread reaction to aspects of the legislation relating to evidentiary certificates and the admissibility of unlawfully obtained evidence. The reactions to these aspects will be summarised in the following paragraphs.

Evidentiary Certificates

2.59 The treatment of evidentiary certificates is dealt with under two headings; evidentiary certificates issued to Telecom employees and the proposal to extend their issuance to law enforcement agencies.

Evidentiary Certificates - Telecom

2.60 The Telecommunications (Interception) Amendment Act (No.2) 1985 amended the Act in two main respects. In relation to evidentiary certificates, it enabled formal evidence of acts done by Telecom employees in enabling members of the AFP to execute an interception warrant to be given by certificate in court proceedings. Strict proof of actions taken by Telecom employees would require those employees to give evidence in court. Telecom management was advised by the A.T.E.A. that employees were unwilling to give such evidence because public identification of their involvement in narcotics interception would cause fear for their own safety, that of their families and that of their fellow workers.[22]

2.61 To assist Telecom employees and avert possible industrial problems, the 1985 amendment Act, provided that evidence of acts performed by Telecom employees to enable the execution of an interception warrant could be given by a certificate signed by the Managing Director of Telecom. The A.T.E.A. welcomed the introduction of the evidentiary

certificate, as it meant that Telecom, rather than an individual officer, would accept responsibility by certifying that a legal interception had been properly executed.[23] The certificate is conclusive proof of the matters contained therein, which are matters of formal evidence only and do not go to any substantial issue before the court.[24] (The Committee understands that the AFP have mechanisms in place to test and prove that interception connections have been made to the numbers specified in warrants).

2.62 Under the subject Bill, proposed section 6C which further amends section 25A, maintains that it is still only intended that evidentiary certificates be issued to Telecom employees.

2.63 Proposed section 6C provides that the Managing Director of Telecom may issue a certificate in writing, (evidentiary certificate), signed by himself setting out such facts as he considers relevant with respect to acts or things done by, or in relation to, officers of Telecom for the purpose of enabling a warrant issued under section 20, 33, or 44 to be executed. This certificate would be received in evidence in proceedings as referred to in proposed sub-section 7AB(1) without further proof, and would be, in such a proceeding, conclusive evidence of the matters stated in the document.

2.64 When introducing the provision for an evidentiary certificate in 1985 the Attorney-General said:

> The Government recognised that there was an objection to a prosecutor seeking to establish, by certificate or averment, an element of the prosecution case going to the conduct of the accused. However, proof that a warrant was executed strictly in compliance with its terms is a purely formal matter. Further, proving compliance by certificate would not conflict with the recommendations of the Senate Standing Committee on Constitutional and Legal Affairs. That Committee has taken the view

that Parliament should enact legislation to ensure that averment provisions are only resorted to by prosecutors where the matter which the prosecution is required to prove is formal only and does not relate to any conduct on the part of the defendant.[25]

2.65 Support for the introduction of evidentiary certificates was given in 1984 by Mr Frank Vincent, Q.C. [as he then was] in his report 'Review of Matters Affecting Telecom'.[26]

Evidentiary Certificates - Law Enforcement Agencies

2.66 It was suggested to the Committee in evidence that proposed section 6C 'Evidentiary Certificates', be extended to include under its ambit, law enforcement agencies. It was considered by some witnesses that the extension of this provision would save valuable 'monitor' manhours, currently wasted by the requirement for the monitors to appear in court. One such suggestion for the extension of this provision came from the AFP:

> The Bill is not as comprehensive as we would have hoped and requires further amendment to include a provision in sub-section 6C for a rebuttable presumptive evidentiary certificate to provide a method of proving the monitoring of specific intercepted conversations before the court, without the need to call all the monitors. The rebuttable presumption would be the acceptance of the facts contained in the certificate as prima facie evidence of the monitoring of the conversation unless challenged by the defence.
>
> Experience has shown that in the majority of instances there is no challenge to monitors giving details of the interception of conversations. ... The cost of attendance and the dislocation to the Special Projects Branch whilst these members are away at court, is quite substantial. Provision of a certificate on the statement of a monitor, which permitted the court to accept the contents of the statement as prima facie

evidence, unless challenged, could result in significant savings in court time as well as to the AFP.[27]

2.67 An AFP witness, in evidence to the Committee, explained the current procedures for presenting, in court proceedings, evidence gained from approved telephone interceptions:

> We have had a number of operations that have run on for many months and given the resources we have dedicated to this exercise, at one stage or another throughout an operation, most of the people involved in this particular activity would have been involved in the interception, the adjudication process of the product and the dissmemination of the product.
>
> The end result of that has been that we have almost had to close down the remaining 13 or 14 operations that we had running because all of our people have had to go to court for what can be described as a very formal type of presentation of evidence, saying: 'Yes, I did this on such and such a day; I made the connection and I made that entry in the log'. It has involved nothing more and no cross-examination - it has been purely a formal submission of evidence.[28]

2.68 The AFP witness went on in his evidence to state that the evidence provided by AFP monitors was challenged 'on very few occasions':

> I think it is fair to say that perhaps initially the challenges came but, as time has gone on, there have no longer been real issues from the point of view of the defence counsel.[29]

2.69 The AFP, although suggesting the use of evidentiary certificates for their operators did not argue for the certificate to be conclusive:

> [W]e are saying that we do not want a blanket right to do this; we are saying that if there is a request by defence counsel for a witness, we should and would make that

> witness available. However, on those occasions where there is no such request, we would like to see our suggestion picked up as a satisfactory means of catering for a problem at a time when resources are an important issue.[30]

2.70 A witness giving evidence on behalf of the Australian Civil Liberties Union considered while under questioning from the Committee, that the AFP's suggestion that they be able to present an evidentiary certificate during a trial was a 'sensible idea', 'if the defence could challenge it'[31]

2.71 The position of the Attorney-General's Department was clearly stated by a Departmental witness in evidence to the Committee:

> Strange as it may seem, we do not really like giving evidence by way of certificate. I say strange because there is provision in the legislation for some evidence to be given by certificate ... When you get the AFP monitors and so forth going to court they are giving evidence about the integrity of the system and the individual interception in order to establish that the material put before the Court is reliable and should be relied upon. We appreciate that it uses up AFP resources but it was our assessment that it was not really appropriate for information of that kind to be conveyed to a court by certificate, ... we can, without involving Telecom workers, produce evidence from the AFP that establishes the chain for the interception without any missing links. The evidence of Telecom employees is simply, as it were, an additional safeguard at one point along the chain. On that basis the Government was prepared to accept that that evidence could be given by a certificate.[32]

2.72 The conclusive nature of proposed sub-section 6C(2), if it were extended to law enforcement agencies, has drawn an adverse reaction in evidence. For example the Victorian Bar stated in their submission:

The Bill should provide that a certificate in a prescribed form tendered to a court be only prima facie evidence that the conditions precedent to the admissibility of the evidence as required by the Act have been complied with. It must not be a conclusive certificate under any circumstances. Such a certificate should be admissible only where objection is not raised by the party against whom the information is sought to be led. Such a certificate would obviate the necessity of calling a large number of witnesses who would otherwise be necessary to establish the various phases of the intercept and prove the accuracy of the tape recording or transcript. We have had experience of cases in which this task has been exceedingly difficult and unnecesarily complicated because of the lack of co-operation which existed between various Government Departments and occasionally between management and staff within a Government instrumentality.[33]

2.73 It was further argued by Senator Bolkus that:

The 'conclusive' provision, as proposed will prevent the defendant from going beyond the certificate. Such changes in the onus of proof have been criticised in the 1982 Senate Constitutional and Legal Committee report on the onus of proof, and in the 1985 Australian Law Reform Commission report on Evidence.[34]

2.74 This was further supported by the ALRC:

The fact that those certificates are said to be conclusive of the matters to which they relate, as Committee members will be aware, is contrary to the firm recommendation of the Senate Standing Committee on Constitutional and Legal Affairs on evidentiary and other burdens of proof.[35]

Admissibility of Evidence

2.75 The Committee received submissions commenting on aspects relating to the admissibility of evidence.

2.76 The ARLC welcomed the general thrust of proposed sub-section 7AA(1) which, in conjunction with section 7AB(1), would clarify the admissibility of evidence obtained through interception of telecommunications in court and tribunal proceedings.

2.77 In evidence an ALRC witness, said in regard to evidence obtained by illegal interception, that:

> I think the Commission would have taken a more liberal and somewhat less restrictive approach to that, and would have treated evidence obtained by unlawful telephone tapping in the same way as the law treats evidence that has been obtained through any other kind of illegality.[36]

2.78 The NCA's position was:

> The Authority does not support removing the question of admissibility of unlawful evidence from the ambit of common law.[37]

2.79 This opinion was supported by the Victorian Police Association:

> We believe that the Common Law principles as applied by the Trial judge who has heard all the evidence in the case should prevail as they do at the present time.[38]

2.80 The New South Wales Labor Lawyers witness stated:

> The submissions of the NCA and the New South Wales Police seeking retention of the common law are strongly opposed - at common law unlawfully obtained evidence is prima facie admissible[39]

2.81 This witness went on in explanation of his opposition:

> ... it is very difficult to have excluded illegally obtained evidence at the common law. The burden of proof lies with the accused, the burden of proof does not lie with the police. It is important that there be a general prohibition on illegally obtained evidence.[40]

Admissibility of Evidence in Disciplinary Proceedings

2.82 The purpose of proposed section 7AB, according to the Attorney-General's Department, is to make lawfully intercepted information inadmissible in evidence in any proceedings other than proceedings of the kind referred to in proposed sub-section 7AB(1), and to make information intercepted in contravention of the Act inadmissible in any proceedings except for the purpose of establishing the contravention. Proposed paragraph 7AB(1)(g) provides that lawfully intercepted information may be admitted in evidence in police disciplinary proceedings. Proposed paragraph 7AB(1)(h) makes such information admissible in evidence in 'a proceeding against an officer of the Commonwealth, of a State, or of a Territory for misbehaviour or improper conduct, not being a proceeding by way of prosecution for an offence.'[41]

2.83 In its consideration of proposed section 7AB of the Bill, the Committee received evidence which suggested there were concerns with the provisions contained therein. According to at least two organisations, the ALRC and the New South Wales Police Association, the ambit of the provisions of proposed section 7AB should be reconsidered.

2.84 For example, the ALRC questioned the proposal to extend the ambit of the provisions to what are broadly called disciplinary proceedings not involving a prosecution for an offence, arguing that 'imposing restrictions on the use of information obtained by telecommunications interception promotes

adequate recognition of the extremely intrusive nature of such interception.'[42] Further, the Commission argued that:

> To limit the availability of tapping to a small class of offences, but then to allow information so obtained to be used in a wide variety of circumstances, including in evidence in disciplinary proceedings which carry no custodial penalty is inconsistent.[43]

2.85 This issue was taken up by the New South Wales Police Association:

> we do note that in the proposed Bill there is a Clause 7AB which deals with evidence and that apparently, if the Bill is assented to, would allow intercepted communications to be admitted in evidence at disciplinary proceedings ... several of our members have been before the Police Tribunal, have been subject to disciplinary proceedings, and have had telephone interceptions by the AFP admitted in evidence ... We wonder, notwithstanding the main clause, clause 7, which outlines the case of telephone taps being placed in position because of offences carrying a penalty of three years or more, just what it was hoped could have been achieved with disciplinary proceedings. With wry humour we noted this morning that Mr Avery, for example, suggested that there would not be fishing expeditions. It seems that apparently that is exactly what some of our members have been subject to and have fallen into the net of a bigger fishing expedition. There have been taps put in place. Some of our members have been caught by those taps and they have faced disciplinary proceedings and had that evidence placed before those proceedings.[44]

2.86 In short, the New South Wales Police Association argued, if lawfully intercepted information is to be admissible in police disciplinary proceedings for activities or offences which are unrelated to the purposes for which an interception warrant was issued, then similar evidence should also be capable of admission

in proceedings against all levels involved in the administration of criminal justice, including the judiciary and the executive.[45]

2.87 The Committee sought the Attorney-General's advice as to whether this is the intention of this section, and if so, how the intention is to be effected. Further, in relation to proposed paragraph 7AB(1)(h), the Attorney-General was asked to provide a definition of 'misbehaviour or improper conduct'.

2.88 The Attorney-General provided the following advice on the intention behind proposed paragraph 7AB(1)(h) and how the intention is given effect.

> Section [paragraph] 7AB(1)(h) refers to a proceeding for misbehaviour or improper conduct against a Commonwealth, State or Territory officer (other than a police officer). The term 'officer' in relation to the Commonwealth or a State or Territory is defined to include (a) a person holding, or acting in, an office (including a judicial office) or appointment, or employed, under a law of the Commonwealth, State or Territory, as the case may be, and (b) a person who is, or is a member of, an authority or body established for a public purpose by or under a law of the Commonwealth or of the relevant State or Territory or who is an officer or employee of such an authority or body [see proposed amendments to s.5(1) and proposed s.5(3)(ac)].
>
> The intention was that, just as proposed s.8AB(1)(g) would allow the admission of intercepted information in police disciplinary proceedings, s.7AB(1)(h) would allow the admission of intercepted information in non-criminal proceedings for misbehaviour or improper conduct against other public officers involved in the administration of justice, including the judiciary and public servants.
>
> However, as drafted the provision would not cover statutory office-holders. This is because of the definition in the Bill of the word 'proceedings'. A 'proceeding' is defined as a proceeding or proposed proceeding in a federal court or in a court

of a State or Territory or before a tribunal in Australia, or before any other body, authority or person in Australia having power to hear or examine evidence (see ss.7AB(9) and 7AA(17)). Whilst statutory office-holders are commonly subject to removal from office by the Governor-General for misbehaviour, that action would not constitute a proceeding before an authority or person having power to hear or examine evidence.

In view of this I would propose that the legislation be amended to cover all statutory office-holders by, for example, inserting a provision in proposed s.7AA permitting disclosure of intercepted information to an inquiry into alleged misbehaviour or improper conduct by a statutory office holder.[46]

2.89 In relation to the definition of the phrase 'misbehaviour or improper conduct' as it appears in paragraph 7AB(1)(h) the Attorney-General said:

The term 'misbehaviour' is frequently specified in legislation as a ground for removal from office of judges and statutory office-holders. Legislation of this kind never attempts a definition and nor has 'misbehaviour' been precisely defined by judicial decisions. The concept is, of its nature, almost incapable of precise definition. In an opinion of 18 October 1982, Sir Maurice Byers QC (then Solicitor-General) said 'Where an office is terminable for misbehaviour, what must be sought is misconduct in the office or such behaviour outside it as establishes the incumbent's unfitness for the office'. More recently, the Parliamentary Commission of Inquiry has given a similar meaning to 'misbehaviour' for the purposes of s.72 of the Constitution.

The concept of 'improper conduct' is in substance much the same as that of 'misbehaviour'. However, 'improper conduct' is the term most frequently used in public service disciplinary provisions (see, for example, s.56(d) and (e) of the Public Service Act 1922). It is for this reason that the term is included in proposed s.7AB(1)(h).[47]

One Party Consensual Interception

2.90 Some submissions suggested a requirement for a provision to be inserted into the Bill allowing for one party consensual interception. For example, the AFP submission refered to a situation where one party in a telephone conversation consents to the telephone call being taped:

> The advantages of such a provision would be in the higher profile emotive issues such as kidnapping or extortion and in drug investigations when an informant or undercover person is being contacted by alleged offenders. A provision similar to that contained in Section 219B of the Customs Act 1901 would facilitate police investigations.[48]

2.91 The ALRC recommended by majority that one party consensual interception should be permissible:

> The opportunity should be taken to amend the definition of 'interception' (s6(1) of the Act) to remove the difficulty that presently exists in relation to participant monitoring: under s6 as it presently stands, it is arguable that it is the person actually speaking at the time whose consent is required, not his or her hearer.[49]

2.92 The Attorney-General's Department provided the following advice on the current legal position relating to one party consensual interceptions.

> In R v Padman ((1979) 25 ALR 36, 38) it was held , with respect to a provision of the Telephonic Communications (Interception) Act 1960 essentially identical to s.6(1) of the 1979 Act, that in a telephone conversation, the person making the communication is not necessarily the one who makes the call. Rather, it is the person speaking at any paticular time. In a situation where one party (only) to a telephone conversation has knowledge that it is being listened to or recorded by a third person in its passage

over the telephone system, there is an illegal interception of what the other party says during the conversation.

The result is that it is not unlawful for the caller to record his end of a telephone conversation, but it is unlawful to record the replies without the knowledge of the person making them.

This contrasts with the position under the various listening devices legislation of the States and the Commonwealth 'where participant monitoring' (that is, where one party to a private conversation uses, or consents to the use of, a listening device to record it without the consent of the other party) is generally permitted. The position under the Interception Act also contrasts with that under the American and Canadian legislation on telephone interception. In the former case, Title III of the Federal Omnibus Crime Control and Safe Streets Act of 1968 permits interception of a conversation for official purposes where one of the parties to it has consented to the interception; private interceptions where one party consents are also permitted unless the interception is for a criminal, 'injurious', or tortious purpose. In Canada, the prohibition on interception of a private communication does not apply to 'a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it' (s.178.11 of the Criminal Code).[50]

2.93 A peripheral issue relating to one party consensual interceptions was that brought to the Committee's attention by Australian Airlines, Ansett Airlines, Qantas and the Victorian Totalizator Agency Board (Victorian T.A.B.). This issue was recorder-connector devices used by all the above organisations.

2.94 The organisations identified made submissions to the Committee and gave evidence on the difficulties associated with the requirement to operate Telecom recorder-connector devices.

2.95 The Australian Airlines requires that the authorisation to install and use intercept equipment be given in advance of a particular requirement, and remain in force for an unlimited period of time. Secondly they require that the recording be deemed admissible in evidence.[51]

2.96 Ansett Airlines requested that the reasonable and proper use of established procedures to combat the particular type of crime to which their industry is so vulnerable does not become unlawful by the operations of the proposed Bill. Secondly as with Australian Airlines, they required that the evidence gathered is not deemed inadmissible as a result of the Bill.[52]

2.97 The Qantas submission related to surveillance aspects involving crimes against aircraft, passengers and crew. They submitted that private sector instrumentalities such as themselves should be able to secure approval in advance to effect surveillance of telephone communications.[53]

2.98 The Victorian T.A.B. submitted that for the T.A.B. to have to use pip tone recorder connectors serves no useful purpose and is, indeed, onerous given the cost of providing the connectors and the propensity of the connectors to interrupt calls, break down and give rise to disputes with customers. The Victorian T.A.B. recommended inter alia:

a. that any proposed amendments to existing legislation take into account the T.A.B.'s current practice of recording all conversations with its Telephone Betting customers with the full knowledge of those customers and excuse it from compliance with any restrictions or requirements which may be adopted in respect of the recording of telephone conversations;

b. that the present interpretation of legislation and government policy by Telecom be revised to allow the disconnection of pip tone recorder connectors by the T.A.B.; and

c. that, in the event that some form of warning is still required to be given by the T.A.B. to its Telephone Betting customers of the fact that it is recording their conversations, the stipulation of pip tone recorder connectors be relaxed in favour of an alternative which better suits the T.A.B.'s needs.[54]

2.99 On request from the Committee Telecom addressed themselves to the specific problems and requests outlined above. Telecom provided the following advice:

> Concerning the matters raised by the airlines, it is Telecom's understanding that the recording of telephone conversations with equipment authorised by Telecom (see section 6(2) of the Interception Act) does not constitute an interception. Therefore the evidence provisions in the draft Bill would not apply ie the airlines would not be prevented from making use of the recorded conversations in court proceedings.
>
> It is understood that the Committee has also received a submission on the matter from the Victorian TAB. Representations were received from the TAB earlier this year to have the pip tone deleted from its recorder connectors as it was distorting the recording of betting transactions. The T.A.B. was advised that if the pip tone was deleted it would not be a contravention of the Interception Act if customers were aware the conversations were being recorded. However, the equipment would be unauthorised (by Telecom) and Telecom, in accordance with the 1965 Government decision, and its powers under the Telecommunications Act and By-laws, would be obliged to disconnect the equipment.

> Telecom has not received any similar representations as it now supplies equipment which does not record the pip tone - it is only heard by the caller. The TAB, Vic has older equipment which records the pip tone and it is apparently unwilling to invest in the new equipment.
>
> A solution to the TAB situation would be for the Government to authorise Telecom to provide recorder-connectors without pip-tone in situations where it is satisfied that callers were aware that their conversations would be recorded. However, Telecom would prefer that the matter be resolved in the context of other important related matters, for example, whether acoustic recording of telephone conversations (without the knowledge of the other party) should be illegal and the Law Reform Commission recommendations concerning participant monitoring.[55]

The Form of the Legislation

2.100 An opinion expressed frequently to the Committee was that the legislation covering the interception of telecommunications is complex, convoluted, obtuse and confusing. The AFP advised the Committee:

> The Bill is, however, in our view, unnecessarily complex and needs to be simplified. The convoluted construction, and the language used, make it very difficult to determine the precise objectives of the various parts.[56]

2.101 This was a widespread sentiment, expressed in other submissions as follows:

> Senator Bolkus
>
> the extensive amendments proposed for this Act will see it rival the Taxation Act for complexity and obtuseness.[57]

The Victorian Bar

> We have already observed that the form of the amendments is extremely complex and will inevitably give rise to difficulties in interpretation. ... The amending legislation will obfuscate and confuse readers. We propose that in any future amendments of such substantial nature a new Bill come into existence which will incorporate both the Act to be amended and the amendments (the amendments possibly being underlined) so that new legislative structure can be looked at coherently and in one document. The drafting of this particular Bill appears to us to create enormous difficulties in sorting out not only how things fit together but what is actually intended.[58]

2.102 The witness for the New South Wales Council for Civil Liberties in expressing the concern of her Council stated that 'we are concerned that there should be a new Act that is more intelligible and contains all the powers and provisions.'[59]

2.103 On the other hand, however, the witness for the Law Society of New South Wales told the Committee that from a lawyer's points of view, as a lawyer he found it readable and comprehensible.[60]

2.104 Mr Stephen Mason, Secretary and Director of Research with the ALRC, and an ex-legislative draftsman stated:

> I found the amending Bill difficult to follow. In large part this is because there is not available a paste-up of the Act - a complete reprint of the Act. It would be much easier if one could read the Act as it presently stands and see how the Bill slots into it.[61]

2.105 The A.T.E.A. admitted in evidence to the Committee that they:

> experienced considerable difficulties in comprehending quite what is proposed in the amendments to the Telecommunications (Interception) Act 1979.

> We found the Bill confusing and we would suggest, badly drafted. These problems have compounded the difficulties which are normally experienced by a lay person in understanding legislation. This confusion is to be regretted, especially in such a sensitive area as phone tapping which may lead to significant intrusions into privacy. ATEA believes that the confused nature of the legislation by itself is sufficient grounds to warrant its withdrawal.[62]

2.106 A witness from the Attorney-General's Department acknowledged that he would be 'quite happy to admit that the legislation, if this Bill were to be enacted, would be complex.[63] He went on to state:

> I certainly do not oppose the introduction of a completely new Act. I agree with the suggestion that it would be neater - by the simple arrangement of consecutive numbering it would be a little easier to understand and to find your way around.[64]

2.107 The witness went on to say in answer to a question from the Committee about the basis upon which the Attorney-General's Department and the Office of Parliamentary Counsel decides whether to recommend a new Act, or build on the existing framework:

> Certainly where there is already existing legislation the office seems to work on the basis of amendment.[65]

2.108 To some organisations and individuals, the subject matter of the legislation renders it so sensitive that any possible cause for confusion in relation to matters affecting basic and fundamental issues of privacy cannot be tolerated. On the other hand, some community groups, eg the Supporters of Law and Order and the Concerned Citizens of Griffith, were happy to register their full agreement with the provisions of the Bill, and presumably the intent of the legislation, and the checks and balances it seeks to implement.

Uniform Surveillance Laws

2.109 It became quite clear to the Committee as the inquiry progressed that commonsense dictated that the Act, and the Bill, only legislated for a narrow slice of the general surveillance area. The Committee discovered that there is no consistency or uniformity between state and Federal laws dealing with the field of listening devices. Indeed two States did not have legislation in this area. The Committee canvassed witnesses in regard to the possibility of introducing Federal legislation in respect of all listening devices. The sensitive problem of the Federal Government's constitutional power to legislate with respect to these matters was also examined. The ALRC examined this issue in their Privacy Report No. 22. In their submission to this Committee the ALRC explained that:

> One suggestion that has been made is that the regime under the Telecommunications (Interception) Act 1979 be extended to cover interception by means of devices that do not 'plug into' the system but are, for example, placed on or near a phone. By majority, ALRC recommended against such an extension, in large part because of doubt whether s 51(v) of the Constitution would extend so far. ALRC's view was that such interferences with communications were equally privacy invasive but should be dealt with under listening devices laws. For constitutional reasons, the laws would largely be State laws, except in the ACT. ALRC suggests that the opportunity should be taken to try to achieve unformity in this area. The distinction is constitutional and therefore to an extent artificial. Consideration should be given to the Commonwealth enacting listening devices laws for the ACT in accordance with ALRC 22 recommendations and requiring, under the mechanism proposed in s 43, that State access to telephone tapping be conditional upon similar laws being in force in the State concerned.[66]

2.110 This position was further explained by the Secretary and Director of Research with the Commission, Mr Stephen Mason. In evidence he stated:

> The Telecommunications (Interception) Act, the Commonwealth law, would not prevent a person putting a microphone which could pick up telecommunications messages on to the handset or whatever without getting into the system. That distinction is consitutional, and therefore to an extent artificial. Consideration should be given, we say, to the Commonwealth building into the section 43 mechanism a requirement that appropriate listening device laws, based on the same principles as the principles espoused in the telecommunications laws, be enacted at the State level. It would also involve the Commonwealth enacting itself similar laws for the Australian Capital Territory.[67]

2.111 He went on to say that in his view, other devices like cellular radio and telex services would be capable of being brought within the constitutional provision of Section 51(v):

> So long as there is a radio-type device then that is amenable to control it seems to me under Section 51(v) of the Constitution, in the same way as ordinary broadcasting is amenable to regulation under that power. Without that telecommunications or radio type component, it seems to us that you are outside the area where Section 51(v) operates and you need to rely on complementary State and Territory laws.[68]

2.112 Mr Mason further stated:

> The Commission (ALRC) took the view that it would be a better and surer way of achieving uniformity in this area, to have the States enact legislation on the same basis in those areas where there was not Commonwealth constitutional power - that is outside the area of the service.[69]

2.113 The NSW Council for Civil Liberties considered 'that there should be uniform eavesdropping laws in Australia as there are in Canada and the United States, where there is only one standard to protect the privacy of conversations.'[70]

2.114 The witness for the New South Wales Labor Lawyers commented that the legislation in relation to interception of a telecommunications system should be rationalised to incorporate other Federal legislation touching upon listening devices (the Customs Act 1901 and the Australian Security Intelligence Act 1979). Further, he suggested, a reconsideration of the fundamentals of Section 7(1) is required, with a view to addressing the instances in a significant class of cases involving listening devices and eavesdropping which did not fall within this section but fall within 'the field', but not subject to the applicable State Listening Devices Legislation.[71]

2.115 On the possibility of some type of uniform system being established to enable the interception of personal or business communications generally, Mr Justice Stewart submitted the position of the NCA:

> The Authority does however see merit in a uniform system being established, which would enable communications generally to be intercepted by law enforcement agencies subject again to safeguards by way of judicial warrant and the like. As with telephone interceptions, the Authority considers that such powers should be available directly to it. On the specific question of listening devices, the Authority is currently comtemplating approaching the Commonwealth, State and Territory Governments with a view to the Authority being empowered under the relevant legislation to use such devices.[72]

Safeguards

2.116 Detailed legislative safeguards covering telecommunications interception, as in US and Canadian legislation, were given widespread support, especially by individuals and organisations representing privacy and civil liberties bodies. Some criticism was aimed specifically at the annual reporting provisions, which were not regarded as being sufficiently comprehensive.

2.117 In support of this feeling of frustration, the witness for the New South Wales Council for Civil Liberties said:

> In relation to further objective evidence of how phone tapping and bugging is used, we are all in the dark because there are no public annual reports as there are in the United States and Canada - really detailed statistical reports. I have even attempted to find the annual reports of the South Australian Listening Devices Act, and the uses of that, which is the only listening devices Act which requires an annual report. As far as I can find, and I have been through the parliamentary sources, there is no complete collection of annual reports under that Act, either. .... All we have in Australia are incomplete one-line reports from the South Australian listening devices Act.[73]

2.118 She went on to point out that, unless the provisions of the Bill were enforced the safeguards exemplified by the annual reporting provisions would be useless. In support of this, she cited that under the 1985 amendments to the principal Act a report under the 1985 emergency powers was to be given to the Minister who in turn would table the report in both Houses of Parliament. This has yet to be done, leaving the general public it was argued, in a state of ignorance as to how comprehensively the current powers are being used.[74]

2.119 Questioned by the Committee on the proposed safeguards in relation to warrants, the witness for the New South Wales Council for Civil Liberties stated that 'We really need the sort of detailed warrant procedures that they have in North America. You need to have more detailed warrant procedures so that there will be a paper trail for the administration. ... The Auditor-General should be able to report directly to Parliament; he should have to; he should be required to report direct.'[75]

2.120 The ALRC pointed out that:

> Proposed s 6D, in conjunction with the proposed s 27A, will introduce the requirement that the Minister administering the Act (Attorney-General) table in Parliament reports on the number of interception warrants issued and the use made of the information thus obtained. ALRC supports this as it accords with recommendations in ALRC 22 para 1167.[76]

2.121 Mr Mason (ALRC) put to the Committee that having to approach a Judge and requiring him or her to be satisfied of certain things was in itself a safeguard. Under questioning, however, he admitted that he had heard of no cases in Australia where an application to a Judge for a warrant had been rejected.[77]

2.122 The Committee found general support for the requirement that an application for a warrant must convince the judge as to whether interception is an appropriate tool. The New South Wales Council for Civil Liberties proposed a number of procedures in relation to warrants, recommending that Australia adopt the practice that has worked in the US and Canada for 15 years. In answer to a question from the Committee as to whether she thought that the procedures she was recommending would slow the process down leading to further complaints about delays in implementing warrants, the witness replied:

> I should not think so. If the police say that they have got this information when they ask for a warrant, all the warrant procedures would require was that they have it in writing and that they give evidence on oath to the judge. A lot of the warrant procedures that we are concerned with involve looking after the documents afterwards and looking after the tape material that is obtained; making sure that it is put in safekeeping and reporting back to judges - things like that. The problem between Telecom, the Federal Police and the State police is something that exists within their own organisations.[78]

2.123 She went on:

> The police have to understand that they are operating in a criminal system where there should be no less a standard for a phone tap than there is for a search warrant. When they operate in the criminal area they have legal advisers and people very experienced in drafting affidavits. They should not expect to have a lesser standard in their telephone tapping.[79]

2.124 Under further questioning from the Committee about the shortcomings in the procedures that are used by the AFP and the Federal Court Judges who are administering the existing system the witness for the New South Wales Council for Civil Liberties asserted that:

> There is not sufficient documentation in the application before the Judge to allow people to challenge the warrant afterwards or to allow the Auditor-General to review the whole basis of the granting of the warrant ... This procedure for applying for a warrant is a matter of routine. I do not think that would increase the time taken by the police to obtain the tap.[80]

2.125 The ALRC notes 'that proposed s 43 simply requires that the law of the State make "satisfactory provision" for safeguards'. 'It is arguable', they said, 'that the ability of the State concerned to implement those safeguards satisfactorily is not fully covered and it may be desirable to have the Bill expressly advert to this matter.'[81]

2.126 ALRC support 'the proposal that their compliance with safeguards [ie, States] provided by their laws be monitored by an independent authority. This will go some way towards allaying the reasonable fears of citizens regarding the potential for misuse of private information.'[82]

2.127 Safeguards and protections considered necessary by the Committee are considered in more detail in Chapter 6.

Warrants

2.128 One of the recommendations of the Stewart Royal Commission was that the power to issue warrants should be restricted to Judges of the Federal Court and of the Supreme Courts of the States and Territories.[83] The Bill picks up this recommendation, and requires that warrants be issued by Supreme Court Judges in the case of State and Territory police forces and the State Drug Crime Commission and by Federal Court Judges or Supreme Court Judges in the case of the NCA.

2.129 There was, however, some evidence in opposition to the proposal to extend the warrant-issuing power beyond Federal Court Judges. It was suggested in one submission that it should be limited to Federal Court Judges for the following reasons:

a. It will ensure efficient reporting of warrants granted, and ensure uniformity in the administration of and compliance with the rules;

b. State judges hearing applications under Section 7AC(4) to have phone tap material excluded are less likely to find fault with the issuing judge if it is a fellow state judge;

c. The more judges with issuing power, the more applicants for warrants will go 'judge shopping' for one likely to issue a warrant;

d. The National Crime Authority would be able to shop interstate since a judge in one State will be able to issue a warrant for an interception in another (proposed Section 33(8)), and

e. The States will be able to select 'eligible judges' (proposed Section 42) for political reasons.[84]

2.130 The New South Wales Council for Civil Liberties was concerned about State Judges having certain powers in relation to the issuing of warrants, because there are so many State Supreme Court Judges. 'Federal Court Judges are most unlikely to be involved in the criminal cases that result from the issue of their warrants, so they are not likely to be reviewing themselves, whereas the State Judges are.'[85]

2.131 The Committee attempted to clarify the Council's concern and questioned whether the competence or integrity of State Judges was at issue. The witness, for the Council, responded that State Judges are:

> ... a bit closer to the criminal law system, that is all. Unless you have a proper system that ensures uniformity of decision making - and I would say that we would need the more detailed system of issuing warrants - there may be differences. They may not be as uninvolved as the Federal judges definitely are.[86]

2.132 The witness for the Law Society of New South Wales stated his Society's position:

> phone taps can only be allowed by warrant from a Supreme Court or Federal Court Judge, upon affidavit or other sworn evidence of a police officer of the rank of sergeant or above, who has personal knowledge of the matters deposed to.[87]

2.133 He further stated:

> all warrants should be returnable within such period to be stipulated by the issuing Judge, being a period less than twenty eight days, and should not be renewable without fresh cause being shown.[88]

2.134 In regard to the criteria to be applied by a Judge in considering whether or not to grant a warrant, the Law Society of New South Wales witness said a warrant should include:

(i) the likelihood that a warrant will produce evidence of a serious criminality;

(ii) the potential for hardship that the granting of a warrant may cause to persons other than the suspect.[89]

2.135 The ALRC generally supported the measures proposed in the Bill to revise the method of application for warrant,[90] and contended that:

> considerations, including the appropriateness of the method of investigation, the effect on individual privacy and the gravity of the offence, and the availability of other evidence should all be matters that are taken into account by the Judge who is asked to issue the warrant. The fact that it is an offence of seven years or more is not of itself enough to authorise the tap.[91]

2.136 The Law Council of Australia contended that the proposed amendments to Section 20 which would require the Judge issuing the warrant to have regard to any prejudice to the conduct of the relevant investigation and to the availability of alternative means for obtaining the relevant information, did not go far enough in the protection of individual privacy. In particular, it continued, it fails to require the Judge, as proposed by Commissioner Stewart in his fourth recommendation, to consider the gravity of the matters being investigated and the extent to which the privacy of any person is likely to be interfered with. There is, it was argued, a need for an explicit procedural protection for the evident legislative presumption favouring privacy of the individual.

2.137 Reflecting this argument, it was submitted by the Law Council of Australia that individual privacy requires express consideration both by the applicant for a warrant and by the Judge considering whether or not to issue one. It ought to be a

specific statutory condition of the power to issue a warrant under Sections 20, 33 or 44 of the Act as amended that the issuing judge consider the extent to which the privacy of any person is likely to be interfered with (balanced of course against the gravity of the offence).[92]

2.138 The Law Council of Australia further submitted that:

> It is evident from the provisions of the Act that applications for warrants will be made ex parte. There is a risk that in the absence of some representative of the public interest in privacy, their issue could tend to become routine. The interests of persons whose conversations are to be intercepted are not represented on such an application except to the extent that the Judge himself may raise questions about the basis upon which the warrant is sought. It is however preferable that the Judge not have the sole responsibility for indentifying and bringing to his own consciousness those matters which in the interests of individual privacy might militate against the issue of the warrant.
>
> Under Danish legislation dealing with the interception of telephone conversations as passed by the Danish Parliament on 6th June 1985, provision is made for the appointment of an attorney to safe guard the interests of the suspect prior to the issue of a warrant. The attorney is entitled to familiarise himself with the material held by the police and may obtain a copy of it. He is however prohibited from divulging such information and from contacting the suspect.[93]

2.139 In summary, the Law Council of Australia recommended that:

> It ought to be a specific statutory condition of the power to issue a warrant under Sections 20, 33 or 44 of the Act as amended that the issuing judge consider the extent to which the privacy of any person is likely to be interfered with. (Balanced of course against the gravity of the offence).

> Upon an application for the issue of a warrant there should be provision for representation of the public interest in privacy provided that in the case of urgent applications such representation may be deferred to a later more formal application.[94]

Scope of the Warrant - NCA

2.140 In terms of the subject Bill, the NCA argued for the extension to the Authority of the power to seek a warrant for interception for any 'relevant offence' which it is investigating and proposes that consideration be given to the issue of a warrant to intercept the communications over any telephone service of a nominated person suspected of involvement in a serious crime.[95]

2.141 A witness for the New South Wales Labor Lawyers viewed the NCA's proposition with dismay for the following reason:

> If one looks at the definition of relevant offences carefully, one will see that that covers almost any offence involving more than one person and involving telephones and carrying more than a three year goal sentence. It covers dishonesty offences, violence offences and drug offences and that, as far as I am aware, covers all offences, with the proviso only that the offence be of three years imprisonment or more.[96]

Warrants by Telephone

2.142 The proposition to enable a Judge to issue a warrant upon an application made by telephone, by specially authorised members of the AFP, the NCA and relevant State and Territory authorities in circumstances of urgency was generally supported in evidence to the Committee. As the NCA said,

> the ability to approach a judge by telephone to seek approval for the interception of the communications of other suspects could be invaluable in obtaining information at a critical point in an investigation[97]

2.143 The ALRC also supported the proposition of warrant applications by telephone in circumstances of urgency.[98] The AFP, however, does not support the proposition,

> as it bypasses the normal checks and balances contained in AFP telecommunications interception policy.[99]

2.144 Witnesses from the Attorney-General's Department were asked by the Committee 'why in the face of some concerns expressed by the AFP, is the provision to enable warrants by telephone being proposed?'[100]

> The AFP is not the only potential user under the scheme. We are aware of the fact that the AFP is opposed to the obtaining of these warrants by telephone and, in fact, I think we built in a specific provision that will allow it to control this. ... Our other consultations produced a position different from that put forward by the AFP. It is a fairly standard approach now, in most jurisdictions in this country, when creating a warrant obtaining provision, to make some provision for enabling it to be obtained by telephone in emergency circumstances. This is becoming a standard approach to the creation of warrant giving. We felt that although the AFP did not particularly want it, we were faced with a situation where the other potential users of the system did want that kind of provision retained, and, given that it was part of the standard structure, it was not appropriate for us to leave it out.[101]

Interceptions Without Recourse to Telecom

2.145 One of Stewart's recommendations was that a Judge issuing a warrant should be able, in appropriate cases, to authorise a direct interception without recourse to Telecom.[102] This recommendation was not taken up in the Bill. The Government's view is that the powers to be conferred on State authorities and the NCA should be exercisable only through Telecom.[103]

2.146 The arguments for carrying out interceptions without recourse to Telecom were in the main based on two grounds; the need for greater security and the time delay involved in utilising Telecom. However, at least one police force and the NCA believe that they should not have to use Telecom to facilitate an interception but rather they should be given the power in their own right. The Victoria Police stated in their submission that:

> The requirement for the technical steps necessary to enable an interception to be carried out pursuant to a warrant to be only taken by Telecom is not acceptable. Very often major investigations, particularly those into organised crime, need to be carried out with a great deal of security, in order to maintain the integrity of the investigation. Mr Justice Stewart identified the potential for a breach of security where the telephone interception is effected by Telecom staff.(1) He recognised the need for police to be able to effect interceptions independently.[104]

2.147 In further support the NCA stated that:

> the Authority considers that in certain circumstances it should be empowered both to bypass Telecom and to enter premises.[105]

2.148 The New South Wales Society of Labor Lawyers' witness, asserted a contrary position, however:

> I think proposals for by-passing Telecom should be regarded suspiciously and with caution, and they should not be heeded. These things in themselves provide important safeguards in the whole procedure.[106]

2.149 The AFP are empowered under the existing legislation to facilitate their own intercepts without having recourse to Telecom. However, they have rarely exercised this right preferring to use Telecom. In evidence to the Committee, a spokesman for the AFP said:

> I would have to think back several years to the last time we would have done a local interception, that is one not done through Telecom. They are very rare. It is our experience that the Telecom situation is the right way to go. If you go the other way, even on an ad hoc basis, we reckon the resource implications are too great. If you go out into the field and want to do a local one, and to control it in the way that you would need to control it in every aspect then it presents extended problems.[107]

2.150 The A.T.E.A. also asserted a position contrary to that of the NCA:

> the ATEA welcomes the fact that the legislation does not carry forward the Stewart recommendation that law enforcement agencies should be able to place their own intercepts: This is despite the confusion at section 43(2) of the Bill, which makes reference to persons and classes of equipment that may be used in intercepts undertaken by State police forces. It is now our understanding that the intention of the Bill is that only Telecom will undertake intercepts. ...This will assist in the security of interceptions despite the criticisms that have been made of Telecom security by the National Crime Authority and the Victorian Police. Whatever may be ultimately decided by Parliament, we stress that the principle that only Telecom should undertake interceptions should be adhered to.[108]

Life Span of Warrants

2.151 There was support in some evidence for the argument that the proposal in the Bill to reduce the life span of warrants from 6 months to 90 days was inadequate. This support was best summed up by the ALRC who stated:

> In view of the highly privacy-intrusive nature of telecommunications interception and of the need to keep people's privacy interests constantly under consideration,

ALRC adheres to the recommendation in ALRC 22 that 90 days is too long a time for a warrant to be valid. ALRC notes that it is a reduction of the present period by a half, but also that it is at least 30 days longer than the period permitted in other comparable countries. The period should be 30 days.[109]

2.152 An opposing view was put by the NCA:

> Given the level of effort required of investigators in applying for a warrant and establishing an interception, this period [90 days], represents a reasonable compromise. Unless there is some reason to suspect that events will move rapidly, the investigation of serious criminal conspiracy can be expected to take months.[110]

2.153 The Attorney-General's Department's position on the life span of warrants is as follows:

> We felt that six months was too long and virtually everybody who had looked at this particular area was of that opinion. It came too close to giving a sort of carte blanche. It ran too great a risk of intercepting vast amounts of material that were not relevant to the purposes for which the interception was granted. We also felt that shortening the period, as it were, should be a reflection of police ability to work out when their investigations required an interception, both for the purpose of assisting the investigation in ways that other methods could not accomplish and in order to get the maximum assistance. These kinds of approaches would be best served by shortening the period ... In effect, the 90 day period serves reasonably well to pull the period back from that initial six months and yet retain it with sufficient length and flexibility to allow operational efficiency.[111]

Conclusions

Interpretation

2.154 The Committee was impressed by the concern expressed in evidence in relation to the difficulties posed by definitions in the interpretation section of the Bill. The Committee concludes that these difficulties, outlined earlier, must be addressed in re-drafting.

Scope of the Legislation

2.155 The Committee concludes that the scope of the legislation is not adequately defined. The rapid rate of technological change in relation to telecommunications is not adequately addressed in the legislation.

2.156 Whether the legislation should be confined to 'serious trafficking offences' and matters of national security or be extended to cover 'serious offences', is addressed in Chapter 4.

Serious Offences - The Mechanism for Legislation

2.157 The scope of the recommended legislation to cover serious offences is addressed in Chapter 4.

Evidentiary Certificates - Telecom

2.158 The Committee supports the provisions of proposed section 6C which legislates for the use of evidentiary certificates by Telecom employees. The Committee is fully aware that the 'conclusive clause' contained in proposed sub-section 6C(2) removes a defendants ability to rebut the evidence contained in the certificate. However, as the Committee is satisfied that the 'conclusive clause' would not prejudice a defendants case, it recommends that proposed section 6C remain unaltered.

Evidentiary Certificates - Law Enforcement Agencies

2.159 The Committee accepts that significant AFP and court resources are currently consumed in presenting technical evidence on legal intercepts, and that a case has been made to extend the provisions of proposed section 6C. The Committee therefore recommends that the provisions of proposed section 6C be extended to allow law enforcement agencies, empowered to effect telecommunications interceptions, to produce evidentiary certificates in court proceedings. However, the Committee recommends the exclusion of proposed sub-section 6C(2) in respect of its application to law enforcement agencies.

The Form of the Legislation

2.160 The Committee concludes that the Act, and the Bill, are confusing, convoluted and vague in parts. The proposed Bill compounds an already complex piece of legislation.

2.161 The Committee's conclusion in this respect is developed further in Chapter 6.

Uniform Surveillance Laws

2.162 It is outside the scope of this Committee's terms of reference to canvass fully the areas into which federal legislation covering aspects of surveillance might go.

2.163 The Committee addresses this issue in more detail in Chapter 6.

Safeguards

2.164 The Committee concludes that some additional safeguards consistent with administrative efficiency are necessary. These are addressed in Chapter 6.

Warrants

2.165 The Committee by majority concludes that, on the weight of evidence, and to provide as much protection to individual privacy, the power to issue warrants should be restricted to Judges of the Federal Court of Australia.

2.166 The Committee concludes that in urgent cases warrants should be able to be effected by telephone provided consequent justification is provided (see Chapter 6).

2.167 The Committee does not support the proposition that telecommunications interceptions be placed without recourse to Telecom. To have the interception facilitated by Telecom is an important step in the checks and balances of the process. There is insufficient evidence to support a case to the contrary.

Life Span of Warrants

2.168 The Committee concludes that the 90 day life span of a warrant is satisfactory.

Endnotes

1. H.R. Deb. (4.6.86) 4595
2. Paragraphs 2.2 - 2.39 of this chapter unless otherwise stated are based on:

   a. Telecommunications (Interception) Act 1979
   b. Telecommunications (Interception) Amendment Bill 1986
   c. Telecommunications (Interception) Amendment Bill 1986 (Explanatory Memorandum)

3. H.R. Deb. (4.6.86) 4598-4599
4. Senate Standing Committee for the Scrutiny of Bills, Scrutiny of Bills Alert Digest No 11 of 1986 pp12-13
5. Letter to Committee Secretary dated 18 September 1986
6. H.R. Deb. (4.6.86) 4597
7. H.R. Deb. (4.6.86) 4597
8. H.R. Deb. (4.6.86) 4598
9. Submission, Law Council of Australia, No. 42, pp11-12
10. Submission, Law Council of Australia, No. 42, p14
11. Submission, Law Council of Australia, No. 42, pp14-15
12. Submission, Law Council of Australia, No, 42, pp14-15
13. Submission, Law Council of Australia, No. 42, pp24-25
14. Evidence, 364
15. Evidence, p913
16. Evidence, p866
17. Evidence, p928
18. Submission, Law Council of Australia, No. 42, p13
19. Evidence, pp 672-673
20. Exhibit, National Crime Authority, No. 28, p1
21. Letter to the Committee Secretary from the Attorney-General's Department dated 16 September 1986
22. H.R. Deb. (9.5.85) 1980
23. Evidence, p672
24. H.R. Deb. (9.5.85) 1980
25. H.R. Deb. (9.5.85) 1980
26. Review of Matters Affecting the Australian Telecommunications Commission (Telecom), Report to the Special Minister of State, F.H.R. Vincent, Q.C., June 1984, p47

27. Evidence, p62
28. Evidence, pp96-97
29. Evidence, p97
30. Evidence, p97
31. Evidence, p191
32. Evidence, pp18-19
33. Submission, The Victorian Bar, No 39, pp11-12
34. Submission, Senator Bolkus, No 1, p3
35. Evidence, p879
36. Evidence, p879
37. Evidence, p448
38. Evidence, p200
39. Evidence, p905
40. Evidence, p912
41. Exhibit, Attorney-General's Department, No. 30
42. Evidence, p869
43. Evidence, p870
44. Evidence, pp563-565
45. Evidence, pp563-565
46. Exhibit, Attorney-General's Department, No. 30
47. Exhibit, Attorney-General's Department, No. 30
48. Evidence, pp62-63
49. Evidence, pp865-866
50. Exhibit, No 26
51. Submission, Australian Airlines, No. 14
52. Submission, Ansett, No. 11
53. Submission, Qantas, No. 27
54. Submission, Victorian T.A.B., No. 15
55. Submission, Telecom, No. 34, pp4-5
56. Evidence, p57
57. Submission, Senator Bolkus, No 1, p1
58. Submission, The Victorian Bar, No 39, pp6-7
59. Evidence, p812
60. Evidence, p1089
61. Evidence, p881
62. Evidence, p670
63. Evidence, p5

64. Evidence, p7
65. Evidence, p7
66. Evidence, p870
67. Evidence, p887
68. Evidence, p888
69. Evidence, p889
70. Evidence, p812
71. Evidence, p904
72. Exhibit, National Crime Authority, No. 28, p1
73. Evidence, pp817-818
74. Evidence, p819
75. Evidence, pp819-820
76. Evidence, p869
77. Evidence, p884
78. Evidence, p820-821
79. Evidence, p822
80. Evidence, pp822-823
81. Evidence, p868
82. Evidence, p868
83. The Hon Mr Justice D.G. Stewart, Report-Volume One, Royal Commission of Inquiry into Alleged Telephone Interceptions, 30 April 1986, p354
84. Submission, Senator Bolkus, No 1, p1
85. Evidence, p834
86. Evidence, p834
87. Evidence, p1087
88. Evidence, p1087
89. Evidence, pp1087-1088
90. Evidence, p868
91. Evidence, p881
92. Submission, Law Council of Australia, No. 42, pp18-19
93. Submission, Law Council of Australia, No. 42, p19
94. Submission, Law Council of Australia, No. 42, p25
95. Evidence, pp444-445
96. Evidence, p913
97. Evidence, p448
98. Evidence, p868

99. Evidence, p59
100. Evidence, p20
101. Evidence, p20
102. Stewart, Report, p355
103. H.R. Deb. (4.6.86) 4599
104. Evidence, p361
105. Evidence, p448
106. Evidence, p914
107. Evidence, p136
108. Evidence, p672
109. Evidence, p869
110. Evidence, p446
111. Evidence, pp16-17

CHAPTER 3

THE EXTENSION OF INTERCEPTION POWERS TO THE STATES OF THE COMMONWEALTH AND THE NATIONAL CRIME AUTHORITY

Background

3.1 The Commonwealth of Australia Constitution Act, under Part V - Powers of the Parliament, provides the constitutional basis for the power of the Parliament of the Commonwealth to make laws for, inter alia, 'postal, telegraphic, telephonic, and other like services'.[1] Under this head of power, the Parliament legislated in 1960 to prohibit interception of telephonic messages in their passage over the telephonic system controlled by the Commonwealth.[2] The 1960 Act also prohibited communication of intercepted information except in defined circumstances.

3.2 The prescribed prohibitions on the passage of intercepted information were carried forward into new legislation when the 1960 Act was repealed in 1979. The Telecommunications (Interception) Act 1979 prohibited interception of telecommunications except in the performance of normal Telecom duties or, pursuant to a warrant, by officers of the Australian Security Intelligence Organisation or Customs (now the Australian Federal Police).

3.3 The States of the Commonwealth presently do not have the power to legislate with respect to telecommunications interception by virtue of the Constitution. The subject Bill seeks, inter alia, to make interception powers available to the police force of any State or the Northern Territory, the National Crime Authority and, in the case of New South Wales, the State Drug Crime Commission. The Bill reflects Government decisions

following a Special Premiers' Conference on Drugs held in Canberra in April 1985. The States of Queensland, Western Australia, South Australia and Tasmania, and the Northern Territory were all reported to have indicated an interest in seeking the power of interception for their police in the investigation of drug trafficking offences.[3]

The Proposal in Summary - the States

3.4 The Bill proposes to insert a new Part VII into the Act. Under these provisions, the Attorney-General, by notice in the Commonwealth of Australia Gazette, may declare certain police forces to be declared authorities, thereby extending to them interception powers with respect to serious drug trafficking offences against State or Territory laws. Declarations can only follow:

a. a request of the relevant Premier/Chief Minister, and

b. the Commonwealth Attorney-General's satisfaction that the relevant State/Territory has incorporated necessary safeguards into its legislation.

3.5 The necessary safeguards were summarised to the House by the Attorney-General, in his second reading speech, as being provisions for:

a. reporting on the issue and revocation of warrants to the relevant State/Territory Minister;

b. the proper maintenance of records by State/Territory police;

c. the regular inspection of records by an independent authority;

d. the independent authority to report on the extent of compliance with statutory requirements;

e. the destruction of irrelevant records, and

f. regular reports by the relevant State/Territory Minister.

3.6 The Attorney-General assured the House of Representatives that the required legislative safeguards would be at least as stringent as those applying to the Australian Federal Police. The Bill also provides power for the Attorney-General to revoke, on request by a State/Territory, a declaration. Revocation can also occur if the Attorney-General is satisfied that the requirements of the Act, as amended, are not being satisfactorily met.

3.7 The Bill further proposes that a State/Territory seeking the power of interception for its police force must agree to pay all costs incurred in the issuing and execution of relevant interception warrants to its police and in the implementation of relevant interceptions by Telecom Australia requested by its police.

The Proposal in Summary - The National Crime Authority

3.8 Clause 18 of the Bill seeks to insert into the Act a new Part VI, conferring on the National Crime Authority (NCA) powers of telecommunications interception similar in part to those powers to be exercised by the Australian Federal Police. Under the new provisions, the NCA would be able to seek judicial warrant to effect interception where a serious trafficking offence that is a subject of an investigation by the NCA is involved. Before approving a warrant, the NCA must satisfy the issuing judge that:

a. there are reasonable grounds for suspecting that the nominated telephone service is being, or is likely to be, used by a person who is committing or has committed (or is suspected of committing) a serious trafficking offence under NCA investigation, and

b. the information to be obtained would facilitate the investigation and could not be readily obtained by other means, without prejudice to the conduct of the investigation.

3.9 Other safeguards proposed by the Bill in respect of interceptions effected by the NCA include provisions for:

a. the implementation of NCA interceptions only through Telecom;

b. warrants to be issued only in circumstances which do not authorise any entry upon premises;

c. the NCA Chairman to revoke a warrant and cause relevant interceptions to be discontinued as soon as he is satisfied that the grounds for the warrant have ceased to exist;

d. the destruction of all records and copies of intercepted communications not necessary for the lawful purposes of the NCA;

e. the communication by the NCA Chairman to the Managing Director of Telecom of the issue and revocation of each warrant and the provision to the Managing Director of a certified copy of each warrant and revocation;

f. the retention of copies of all warrants and instruments of revocation;

g. reports to the Attorney-General on the issue and revocation of all NCA warrants and on the use of information obtained by authorised interceptions, and

h. an annual report to the Parliament by the Attorney-General on the numbers of warrants issued, and, subject to identifying constraints, the use made of information from authorised interceptions.

The Case for an Extension of Powers

3.10 The arguments in favour of an extension of interception powers to the States and the National Crime Authority are very briefly outlined in Chapter 16 of the Report of Mr Justice Stewart's Royal Commission of Inquiry into Alleged Telephone Interceptions. In asking whether present interception powers are too narrow, Mr Justice Stewart states that the effectiveness of telecommunications interception in the investigation of organised crime 'is no longer seriously questioned'.[4]

3.11 Stewart cites the success of the illegal interceptions of the NSW Police in support of an extension of powers:

> ... information gained from intercepted telephone conversations resulted directly in the apprehension of offenders who may never have been arrested but for the interception of telephone conversations.[5]

A case is outlined in the Report which involved an escaped prisoner serving a life sentence for malicious wounding with intent to murder. NSW Police apparently attempted to recapture

the prisoner several times during his 19 months at large. Illegal interceptions which began 'some eight to twelve months' before the prisoner's recapture eventually resulted directly in his apprehension.[6]

3.12 In his earlier Report of the Royal Commission of Inquiry into Drug Trafficking (February 1983), Mr Justice Stewart also concluded that the powers to apply for an interception warrant, and the circumstances in which interception could be effected, are 'far too narrow'.[7] But following his drug trafficking inquiry, he further concluded that the major value of intercepted information is in the field of police intelligence - 'such intelligence work must be the responsibility of a central intelligence unit with branches in each of the States'.[8] He then argued that State drug intelligence units should be able to apply for warrants to intercept telephones, and that this and other steps would provide 'a further means of compiling a comprehensive intelligence holding on organised criminal activities in Australia'.[9]

3.13 Having made these observations in 1983, Mr Justice Stewart's position further strengthened in his investigations into alleged telephone interceptions. In the concluding chapter of his 1986 Report, he was clearly again persuaded to the view that there is no validity in the present system whereby the power to intercept is limited to the AFP. He now believed that the present system resulted in a cumbersome central administrative system, inherent delays in implementation and a lack of efficiency in access to information. He concluded that:

> The present distinction is arbitrary and artificial. There is no reason why the power to intercept telephone conversations should be restricted to the AFP ... State police forces should also have this power ... It is important that law enforcement agencies should have the capacity to act very quickly to establish a telephone interception in certain cases. It should be made lawful for police themselves to effect an interception without recourse to Telecom.[10]

3.14 In order to assess the extent to which there is a need, perceived by State Governments and Police Forces, for an extension of interception powers, the Chairman wrote, early in the inquiry, to all State Premiers and the Chief Minister of the Northern Territory, and to their respective Police Commissioners. The results are tabulated at Table 3.1. The Committee was surprised at the minimal response to these invitations to contribute to the Committee's deliberations.

3.15 The extension of the power of interception to State police and the NCA was supported by all State police and Police Associations who made a submission or gave evidence to the Committee. An AFP witness stated in evidence that such an extension would be 'a logical extension to the intercept powers which the AFP has had since 1979 ... [these powers] have gone quite some distance to assist us in terms of our needs from a law enforcement point of view. That being the case there is no reason why, in the AFP's point of view, those powers should not be extended to the States and the the NCA'.[11] The witness went on to assert that, based on AFP experience, the extension of interception powers to State police 'would considerably enhance their abilities and their success rates. That would apply to the National Crime Authority as well'.[12]

3.16 The proposal to extend powers was also welcomed by the Victoria Police, who argued in evidence that criminal investigation was a volatile and, if effective, fast moving process. As such, it was asserted, for telecommunications interception to be viable, 'the mechanism employed to obtain the necessary authority, and put the intercept in place, must be practical, efficient and not unduly delayed by cumbersome legal or administrative requirements'.[13] The Victoria Police accordingly recommended to the Committee that they be given the authority to effect interceptions independently of Telecom.[14]

TABLE 3.1

RESPONSES FROM STATE GOVERNMENTS AND POLICE FORCES*

STATE or TERRITORY	GOVERNMENT			POLICE			Remarks
	Submission to the Committee?	Supports Extension to States?	Supports Extension to Serious Offences?	Submission to the Committee?	Supports Extension to States?	Supports Extension to Serious Offences?	
New South Wales	NO (Premier's letter to Prime Minister only)	YES	YES	YES	YES	YES	Late response
Victoria	NO	Not known	Not known	YES	YES	YES	Government acknowledged invitation but declined to submit
Queensland	YES	YES	NO	NO	Not known	Not known	Government declined invitation to appear at public hearing
Western Australia	NO (Premier's letter to Chairman only)	YES (Premier's view)	NO (Premier's view)	NO	Not known	Not known	No Government submission
South Australia	YES	YES, but AFP to conduct	NO	NO	Not known	Not known	Government declined invitation to appear at public hearing
Tasmania	NO	Not known	Not known	NO	Not known	Not known	No Government acknowledgement or submission
Northern Territory	The Northern Territory Government did not make a formal submission to the Committee but wrote in support of all the recommendations of Mr Justice Stewart			NO (Letter to Chairman only)	YES	YES	

* At the direction of the Committee, the Chairman wrote to all State Premiers on 25 July 1986 and the Chief Minister of the Northern Territory on 21 August 1986, and to their respective Police Commissioners on 31 July 1986, inviting them to comment on the Committee's inquiry.

3.17 The NSW Police Commissioner, Mr J.K. Avery, gave evidence in favour of an extension of powers. Questioned by the Committee on this aspect, he asserted the need for interception powers for his Force in respect of 'offences which would not necessarily be happily or competently dealt with using the usual police methods'.[15] This position was endorsed by Sir Maurice Byers in his capacity as Chairman of the Police Board of New South Wales:

> It is our strongly held view that unless telephone intercept powers are made available to police, there will be little significant improvement in the apprehension and successful prosecution of the major figures involved in high level drug trafficking in this State.
>
> It has been demonstrated conclusively both overseas and in Australia that no major investigative authority can operate effectively without access to telephone intercepts.[16]

3.18 The Queensland Government's formal submission to the Committee supported the extension of the power of telecommunications interception to State police forces. But this support was not unqualified; it was asserted simply 'as a general proposition', and then only 'under the most stringent safeguards and for a limited range of criminal activities associated with drug trafficking.'[17] The Queensland Government declined an invitation to have representatives attend a public hearing of the Committee in Brisbane. The Committee was thus unable to test the reasons for the limitations on the Queensland Government's support for an extension of interception powers.

3.19 The South Australian Government was the only other State Government to respond to the Committee's invitation to make a submission. Whilst supporting the extension of the power to conduct interceptions to State police forces, the South Australian Government considered that the Bill should provide for the Australian Federal Police to effect interceptions on behalf

of State Police. The submission argued that '[s]uch a provision would benefit the smaller States which may not have much call to use the telephone interception powers'.[18]

3.20 The Government of the Northern Territory declined to make a formal submission to the Committee, but advised the Committee that: 'The recommendations in Mr Justice Stewart's report of the Royal Commission of Inquiry into alleged Telephone Interception (sic) are acceptable to the Northern Territory Government.'[19]

3.21 The Committee received no response from the Governments of New South Wales, Western Australia or Tasmania to repeated invitations to make submissions on the Committee's terms of reference. The Western Australian Premier did, however, write to the Chairman late in the inquiry to indicate his support for an extension of interception powers to State police. In addition, the New South Wales Premier's Department provided the Committee with a copy of a letter dated 6 November 1986 from the NSW Premier to the Prime Minister indicating his Government's strong support for the extension of powers to State police and the NSW Drug Crime Commission.

3.22 In response to an invitation to comment on the terms of the Committee's inquiry, several organisations argued in favour of the extension of interception powers to State police. The Victoria Police Association, for example, asserted that the concentration of interception powers in the hands of too few law enforcement bodies would constitute a high security risk, given the capacity of organised crime to infiltrate. Their submission continued:

> State Police are required to investigate the bulk of criminal offences in this country. It seems to us that the power of telephone interception should be given to those who are required by the community to investigate serious and violent crime. For security reasons we do not believe that joint operations are always the most efficient way to conduct operations.[20]

3.23 The Police Association of New South Wales did not initially express a view as to whether interception powers should be extended to the States. Its stance was principally that the rights of its members should be protected, whether as implementers or targets of interception. As the Association's President told the Committee:

> We have no policy on it because we have never had to develop one but, as a general feeling, if we are serious about organised crime, I am sure that our membership as a whole feels that it is necessary. If we are really going to attack organised crime, it is a tool of trade, and of course, if criminals can have it, it seems ridiculous to suggest that police should not have it.[21]

3.24 In its submission to the Committee, the National Crime Authority (NCA) did not argue at any length the case for extending interception powers to the States. However, it did concentrate on the extension to the NCA, in its own right, of these powers, and discussed some of the more fundamental underlying principles.

3.25 The NCA's position is unequivocal:

> The Authority has no doubts, based on its own experience and that of others involved in investigating entrenched criminal enterprises, that interception can be a very effective tool, particularly if used with other measures which operate to cut off criminals from support networks and the considerable funds at their disposal.22

3.26 The NCA submission went on to observe that legislators would quite naturally seek to build a sound legal framework of safeguards to protect individual rights, especially in the light of recent events involving the NSW Police. The NCA further observed, however, that legal intercepts, given carefully defined criteria, are less likely to infringe civil liberties than

illegal intercepts (see Chapter 5). Given this, the NCA urged the Committee to give closer attention to illegal interception and the attendant penalties. It suggested, among other safeguards and reporting requirements, an annual report to the relevant Minister from the head of each agency empowered to effect interceptions to the effect that the head was satisfied that the agency had not been involved in illegal intercepts.[23]

The Case Against an Extension of Powers

3.27 The arguments against an extension of powers were put first in evidence to the Committee by the President of the Australian Civil Liberties Union, Mr John Bennett. In stating the nub of his case, Mr Bennett said that:

> The problem is often posed as one of the dilemmas facing any Western country. How can one fight organised crime, the extent of which, as I have indicated, has perhaps been greatly overstated, without unnecessarily invading a citizen's privacy? Put in this way, the problem seems resoluable only by some type of compromise or balanced solution, such as that currently being put forward, I think, by the Federal Government. A limited amount of phone tapping, restricted to the investigation of a few major crimes, is perhaps acceptable if there are extremely stringent safeguards. But unfortunately this reasonable compromise is not really a compromise at all, because physical and other inherent factors virtually preclude any meaningful limitations, and the invasion of privacy is often far greater than at first appears, which is I think evident from the history of the New South Wales police phone tapping. In practice, innumerable innocent people will have their privacy invaded by officials who, as Mr Justice Brandeis said, are at their best men of zeal, well meaning and without understanding, and at their worst susceptible to graft, corruption and extortion. Because of this the proposal to extend phone tapping powers is, I think, quite dangerous.[24]

3.28 Mr Bennett went on to argue that widening police powers might simply increase the level of criminal sophistication, and at the same time move society towards a situation of limited regard for individual rights and liberties. This was particularly dangerous when it involved 'an unnecessary extension of police powers in particular when Federal police already, if they co-operate fully with State police, should be in a position to obtain the information they want in relation to major drug traffickers'.[25] He later returned to this theme, common to submissions opposing an extension of powers:

> One reason the State police seem to want the powers is that there is a lack of co-operation between the Australian Federal Police and the State police and other agencies, due to a desire to retain the integrity of their respective empires.[26]

3.29 In Mr Bennett's evidence, there emerged also a view which starkly contrasts with the view of proponents of an extension of interception powers. This centres on the proposition put that organised crime does exist in Australia, and that it is a major national problem of serious social proportions. In challenging the 'organised crime theory', he conceded that, if society were disintegrating and there were a major crime problem, he 'might support an extension of powers. It is just a question of where to draw the line ... the important question in a democracy is that people who are seeking an extension of state powers should be put very much on their mettle to establish the need for it'.[27]

3.30 The New South Wales Privacy Committee also gave evidence on the extension of powers. The Committee is a statutory authority established by NSW legislation in 1975, to act as a privacy ombudsman independently of government. The Committee did not express a corporate view on whether interception powers should be co-ordinated nationally or extended to the various State agencies. However, a witness from the Committee gave a personal view in favour of a central national authority, 'because it lends some specific focus for control'.[28]

3.31 In its submission, the Privacy Committee queried whether the present provisions for the passage of intercepted information were, in fact, inadequate. It drew the Committee's attention, inter alia, to sub-paragraph 7(5)(b)(i), which provides that the AFP may communicate information obtained through interception 'where the information relates, or appears to relate, to the commission, or intended commission, of an offence against the law of the Commonwealth, or of a State or Territory, being an offence punishable by imprisonment for life or for a period, or maximum period, of not less than 3 years'.

3.32 The Privacy Committee implicitly argued that the use of provisions such as these, combined with improved administrative efficiency in effecting centralised interceptions and communicating resultant information, should obviate the need for an extension of powers:

> ... the issue of inefficient communications between the AFP and State police should be addressed in its own right, not "solved" by giving State police their own privacy-invasive powers.[29]

3.33 The NSW Council for Civil Liberties submitted that the Committee 'should vote to limit, rather than extend, the present phone tap laws, and that it should reject the proposal ... that phone tapping powers be extended to state and territorial police and Crime Authorities'.[30] Questioned on this aspect, the Council's witness referred to the illegal interception activities conducted by the NSW police from 1968, and agreed to the proposition that a State police force would not be as strongly bound by Federal legislation as a national authority:

> ... there is still a fair body of opinion in the New South Wales Police Force that they themselves should choose whether they should obey the law or not.[31]

3.34 Various organisations presented principled opposition to the extension of interception powers. The Law Society of NSW, for example, stated that it was 'against the extension of powers

in principle'.[32] The witness from the Society further asserted in evidence that:

> it is the belief of the Law Society, a long held belief, that police do not exercise the powers they have at the moment, sufficiently resourcefully. The police do have a certain amount of power to follow money trails.[33]

3.35 Philosophical objection to extension was also expressed by representatives of the Australian Telecommunications Employees Association (ATEA), this objection being based on 'a broad philosophy which believes that the right to security and privacy is an essential feature of any democratic society'.[34] States' powers to intercept were opposed by ATEA on the further basis that the great value of interception lay in its unexpected and unknown nature. The extensive application of interception powers would merely force criminal enterprise to seek more secure means of communication. It would also prejudice widespread public trust in the security and integrity of the Telecom network. In condemning a further extension of powers, ATEA observed that:

> The very value of the illegal New South Wales operation was that no one, given the penalties that applied, could have expected that law enforcement officers sworn to uphold the law would break it in that manner.[35]

Summary of the Case for an Extension of Powers

3.36 Arguments put to the Committee for an extension of powers to other law enforcement authorities may be summarised as follows:

a. organised crime does not recognise State borders;

b. telecommunications interception is an essential weapon in the fight against organised crime;

c. interceptions result in arrests which would not be possible otherwise;

d. interceptions provide invaluable criminal intelligence not otherwise available;

e. centralised interception results in delay and inefficiency;

f. action against organised crime must be swiftly executed;

g. extension of powers would remove the cumbersome centralised administrative system;

h. overseas experience demonstrates the effectiveness of interception in criminal investigation and apprehension;

i. central concentration of interception powers is a security risk, in light of the danger of infiltration;

j. State Police conduct most criminal investigations and should therefore have all available techniques to investigate serious crime, and

k. joint Federal/State task forces using intercepts are not efficient or inherently secure.

Summary of the Case Against an Extension of Powers

3.37 Arguments put to the Committee against an extension of powers to other law enforcement authorities may be summarised as follows:

a. telephone interceptions on a wide scale constitute an invasion of the privacy of innocent parties which can never be justified;

b. present legislation permits State police access to information gained from intercepts, through the centralised AFP system and the establishment of joint task forces;

c. the stringent controls under present legislation did not prevent AFP and State police officers from undertaking illegal interceptions;

d. experience abroad indicates that alleged safeguards such as judicial warrants and time limits on warrants have not been effective;

e. an extension of powers, once granted, is difficult if not impossible to withdraw, even if the powers granted are abused;

f. wider interception powers, granted to State police, would seriously prejudice legally protected confidentiality;

g. 'organised crime' does not exist in Australia on the scale argued by the proponents of extension;

h. interception powers, once authorised, may be used for purposes other than those stipulated by warrant;

i. a greater degree of inter-state police co-operation would obviate much of the need for an extension of interception powers;

j. if organised crime <u>is</u> a major national problem, then a centrally co-ordinated national approach is necessary, and

k. if the present legislation, authorising interception by only two agencies, was abused, then the dangers are clearly magnified by extending powers to the eleven agencies.

Conclusions

3.38 By way of prefacing a consideration of the Committee's conclusions on this aspect of its inquiry, the Committee makes the observation that, somewhat surprisingly, little public involvement was evident throughout the inquiry. Extensive publicity has attended the question of telephone interception since late 1983, with the publication in the National Times of purported extracts of transcripts of telephone conversations, and the publication in early 1984 of further transcripts in the Age of Melbourne ('the Age Tapes'). Moreover, the development of the subject Bill and the release of Mr Justice Stewart's Report also generated much media attention.

3.39 At the start of its inquiry, the Committee anticipated that there would be substantial response to an invitation to contribute to the Committee's deliberations. Advertisements were placed in the major metropolitan newspapers in each State capital and in the national press. Furthermore, the Chairman wrote personally to more than 60 relevant agencies, organisations and individuals seeking submissions. These letters went to, among others, Commonwealth, State and Territory Ministers, State Police Commissioners, Police Associations, Bar Associations, Law Societies, Law Reform Commissions and Committees, various Civil Liberties Councils and selected individuals revealed by literature search.

3.40 As the Committee's series of public hearings ended, a total of only 44 submissions had been received. As outlined earlier, of the State and Territory Governments, only South Australia and Queensland made formal submissions (see Table 3.1). The Northern Territory Government declined to submit, but

indicated its support for all of Mr Justice Stewart's recommendations. The Victorian Government declined to make a submission or attend hearings, as did the New South Wales Government.[36] The Premier of Western Australia wrote to the Chairman indicating his support for an extension of powers to the States, but the Governments of Western Australia and Tasmania made no submission, and there was also no direct response from their Police Commissioners.

3.41 As a result, the Committee had to consider a significant devolution of Commonwealth power to the States without the benefit of a considered assessment of the likely position of a majority of the States on the question. Therefore, the Committee had some difficulty in considering whether:

a. State police should have direct power to intercept telecommunications;

b. State Governments should be offered the power to intercept communications;

c. State Governments would seek the power to intercept under the safeguards proposed in the Bill;

d. the conditions proposed in the Bill were acceptable to the States, and

e. the checks and balances considered necessary by the Committee (see Chapter 6) would be acceptable to and implemented by the States in the event of an extension of power.

3.42 Weighing the evidence before it, the Committee was cognizant of the strength of the argument that telephone interception can be, as Mr Justice Stewart reported, 'an essential and cost effective means of combatting organised and drug related crime'.[37] But the opposing view, based on an inherent right to individual privacy from unwarranted intrusion, commands respect. As the Australian Law Reform Commission has observed:

> The privacy of communications entrusted to the national telecommunications and postal services is something which Australians have come to expect; but many would be surprised at the extent to which their private communications can lawfully be intercepted.[38]

3.43 Among the decisions confronting the Committee was the requirement to 'draw the line' in achieving a satisfactory balance between civil liberties and privacy rights on one hand, and the compelling need on the other hand to provide law enforcement agencies with sufficient information to fulfil their roles and functions, particularly in the areas of combatting organised crime in its socially barbarous trafficking in narcotics.

3.44 The Committee saw valid elements in the arguments of both proponents and opponents. Law enforcers must have rapid and early access to available information, consistent with the need to ensure that interception powers are not abused. At the same time, the privacy of communications and the integrity of the telecommunications system must be respected and preserved to the maximum possible extent. But the Committee concluded that this latter aim would be insufficiently and inadequately achieved in the provisions of the subject Bill.

3.45 Privacy rights are not preserved by permitting interception by up to 11 different agencies acting independently, with inadequate central co-ordination, monitoring, scrutiny and auditing. Notwithstanding this reservation, the Committee concluded that some means could be found to permit law enforcement agencies to have access to information relevant to their roles, and sought by them, with, at the same time, essential central safeguards and co-ordination.

3.46 The Committee concludes:

a. that there is a requirement for information from telecommunications interception to be extended so that the State and Northern Territory Police forces, the NCA and the NSW Drug Crime Commission have rapid access to information on serious drug crimes;

b. that the case to extend to the NCA, State and Northern Territory Police forces and the NSW Drug Crime Commission the power to intercept telecommunications has not been made;

c. that essential rights to privacy and to protection from illegal interception and the malicious use of intercepted material are best preserved by restricting to the minimum the number of agencies legally empowered to effect interception;

d. that a Telecommunications Interceptions Agency should be established to carry out all interceptions for the AFP, the NCA, the State and Territory Police forces and the NSW Drug Crime Commission;

e. that all intercepts should continue to be made through Telecom;

f. that the Telecommunications Interception Agency should be established within the AFP as it is best placed to conduct the interceptions for all authorised agencies, and can guarantee a career structure for officers and maximum staff turnover;

g. that each law enforcement agency should retain the full power to select targets, determine priorities, appraise Telecom, prepare draft warrants and approach Federal Court Judges seeking the issue of the warrants;

h. that while the legal right to target interceptions should be extended and decentralised, once the warrant is issued the interceptions should be carried out by a single agency, on a regional basis if economically justified;

i. that the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission should each be offered lines for telecommunications interception on a full cost-recovery basis and each law enforcement body should have the power to determine the priorities for the use of lines rented;

j. that this extension of access to intercepted information to the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission must be accompanied by stringent centrally co-ordinated safeguards, recognising at the same time a requirement for administrative efficiency and the need for a fast-track mechanism for urgent interceptions to exist with subsequent justification, and

k. that an independent Judicial Auditor should provide audit and scrutiny of the process of interception and implementation of safeguards.

3.47 On the basis of these conclusions, the Committee has determined by majority that the Telecommunications (Interception) Amendment Bill is clearly inadequate to meet the needs for which it was proposed. The Committee recommends that the Bill be withdrawn and replaced with legislation drafted in accordance with the principles enunciated in this Chapter and elsewhere in this Report.

Endnotes

1. S.51(v)
2. Telephonic Communications (Interception) Act 1960
3. Hon L.F. Bowen, Attorney-General, as reported in H.R. Deb. (4.6.85) 4595
4. The Hon. Mr Justice D.G. Stewart, Report-Volume One, Royal Commission of Inquiry into Alleged Telephone Interceptions, 30 April 1986, p340 (henceforth cited as: Stewart, Report)
5. Stewart, Report p340
6. Stewart, Report, p154 (See Chapter 4 for further discussion on the extension of interception powers to cover serious offences not necessarily drug-related).
7. The Hon Mr Justice D.G. Stewart, Report, Royal Commission of Inquiry into Drug Trafficking, February 1983, p659 (henceforth cited as: Stewart, Report-Drug Trafficking.)
8. Stewart, Report-Drug Trafficking, p656
9. Stewart, Report-Drug Trafficking, p660
10. Stewart, Report, pp339-340
11. Evidence, p92
12. Evidence, p102
13. Evidence, p361
14. Evidence, p366
15. Evidence, p523
16. Evidence, p545
17. Submission, Queensland Government, No 31, p1
18. Submission, Attorney-General of South Australia, No 28, p1
19. Letter to Chairman from the Chief Minister of the Northern Territory, 27 September 1986.
20. Evidence, p200
21. Evidence, p569
22. Evidence, p441
23. Evidence, p446
24. Evidence, p175
25. Evidence, p182
26. Evidence, p185
27. Evidence, p192-193

28. Evidence, p1081
29. Evidence, p979
30. Evidence, p712
31. Evidence, p826
32. Evidence, p1091
33. Evidence, p1098
34. Evidence, p674
35. Evidence, p675
36. The NSW Government advised the Chairman, by telex on 16 October 1986, that it would 'be in a position within the next couple of weeks to respond'. The Committee was subsequently provided by the NSW Premier's Department with a copy of a letter dated 6 November 1986 from the NSW Premier to the Prime Minister indicating his Government's strong support for the extension of powers to State police and the NSW Drug Crime Commission.
37. Stewart, Report, p326
38. Australian Law Reform Commission, Report No. 22, Privacy, Volume 1 - Background, p343

CHAPTER 4

THE EXTENSION OF INTERCEPTION POWERS TO COVER SERIOUS OFFENCES

Background

4.1 The second part of the Committee's terms of reference, not part of the subject Bill, but which, if enacted, will affect the Act, require it to examine and report upon:

> the recommendation contained in Mr Justice Stewart's report of the Royal Commission of Inquiry into Alleged Telephone Interceptions to the effect that the power of Interception be extended to cover all serious offences.

4.2 In April 1986, at the conclusion of the Royal Commission of Inquiry into Alleged Telephone Interceptions, Mr Justice Stewart recommended inter alia that 'the legislative limitations on the use of telephone interceptions to drug trafficking offences only be removed'[1].

4.3 Following a Special Premiers' Conference on drugs in April 1985, and considering the recommendations in relation to this matter, the Attorney-General sought the views of the States on the question of extending the Act to cover serious offences. The Attorney-General advised the House that he had received the following responses:[2]

a. the Attorney-General of New South Wales verbally advised that his Government 'has not yet made a decision on the question of extending the Act to cover serious offences';

b. the South Australian Attorney-General verbally advised 'that his Government is still considering the matter';

c. the Queensland Attorney-General sent a telex which indicated 'that the Queensland Government does not presently favour an extension of telephone interception powers to serious offences';

d. the Northern Territory Government indicated by telex that 'it supports an extension of interception powers to cover indictable offences', and

e. the Western Australian Premier indicated that his Government 'does not support the expansion of the category of offences to cover serious offences'.

4.4 Early in this inquiry, the Committee sought the views of the States and the Northern Territory on the extension of intercept powers to their authorities and on the extension of powers to 'serious offences'. Letters were written to all State Premiers and the Chief Minister of the Northern Territory, and to their respective Police Commissioners. The lack of response in some cases and the minimal response in other cases frustrated the Committee's attempts to gain an overall view on the support or otherwise for Stewart's recommendation.

4.5 The position of the State and Northern Territory Governments is summarised at Table 3.1. In outline, the Queensland and South Australian Governments do not support the extension to serious offences. The position of the Governments of Victoria and Tasmania is not known. The Northern Territory Government, although not making a formal submission to the Committee, wrote in support of all the recommendations of Mr Justice Stewart. The Western Australian Premier advised the

Committee on the 24 October 1986 that he does not support the expansion of the category of offences as to serious offences. The New South Wales Premier's Department provided the Committee with a copy of a letter dated 6 November 1986 from the NSW Premier to the Prime Minister indicating his Government's strong support for the extension of telephone interception powers to be conducted in relation to other serious criminal offences, and not limited to only drug trafficking offences.

4.6 The police forces of New South Wales, Victoria, and the Northern Territory support the extension to serious offences. The positions of the Queensland, Western Australian, South Australian and Tasmanian police forces is not known.

The Case for the Extension of Powers to Serious Offences

Summary of Mr Justice Stewart's case

4.7 The material obtained by Mr Justice Stewart led to the conclusion that the present legislation governing the interception of telephone conversations is too narrow and the restriction to drug trafficking offences too selective, arbitrary and artificial.[3] This led to the recommendation that the limitations on the use of telephone interceptions, to drug trafficking offences only, be removed.[4] This was not a new conclusion or recommendation by Justice Stewart. In his earlier Report of the Royal Commission of Inquiry into Drug Trafficking, he stated that:

> The main criticism of the present legislation is that the circumstances in which telephone interception may be made are far to narrow. There should be a right to apply for a warrant when it is likely that a criminal scheme or a conspiracy involving organised crime is on foot.[5]

4.8 Justice Stewart bases his argument for the extension of powers to serious offences on the value of interception as an investigatory aid, and the success of interceptions in America which permitted the FBI to penetrate the upper echelons of organised crime. Further, Stewart relies heavily on the success of the unlawful telephone interceptions carried out by the NSW Police, and the role played by telephone interceptions in the identification and apprehension of offenders.[6] Furthermore, it is asserted, interceptions enable crime authorities to build up a significant intelligence data base. As Justice Stewart said in his 1983 Report:

> Although in some cases interception may happen to provide evidence against an alleged offender, its major use is as a means of intelligence-gathering. It is only when that process of intelligence-gathering is completed that the next step can be taken - an operation in which the criminals are apprehended and charged. The right to intercept is an important weapon in the arsenal of intelligence.[7]

4.9 Stewart argues that to confine the use of telephone interceptions to drug trafficking offences is and has always been illogical:

> There are many other offences not associated with narcotic drugs which constitute a grave threat to the community. Indeed the current description used in the Telecommunications (Interception) Act of 'Narcotic Offence' is an offence punishable as provided by section 235 of the Customs Act 1901. That description extends beyond drug trafficking and embraces possession of narcotic substances. Some offences of that type may be of a trivial nature yet interceptions of telephone conversations may be made for the purposes of investigating such offences while offences such as police corruption, kidnapping, murder and other crimes of violence do not attract the provisions of the Act.[8]

4.10 Further, Stewart contends, the restrictions that apply to the Telecommunications Interception Act do not apply under the Listening Devices Act, 1984 (NSW). Under that Act a warrant may be obtained for a prescribed offence, which means an offence punishable on indictment, or an offence of a class or description prescribed for the purposes of the Act. Mr Justice Stewart's assertion is that the potential for invasion of privacy and intrusions upon personal liberty arising from the various State legislations eg Listening Devices Act (NSW) is far greater than that possible if the powers were extended under the subject Act.[9]

Summary of Other Organisations/Individual Cases

4.11 Typical of the response for the proposal was that of the National Crime Authority which was established expressly to combat sophisticated and entrenched organised crime. Its operations, however, are confined by legislation restricted to 'narcotic offences'. In evidence to this Committee representatives from the NCA stated:

> Confining authorised interception to drug crimes is primarily based on the belief that drugs constitute a grave threat to society, and that the threat to individual privacy represented by telephone interception is an acceptable price for society to pay to combat drug crime. Allied to this central belief are two other elements; first, the view that drug dealing is both a characteristic activity of, and major source of funds for, organised crime; and secondly, that it is very difficult (and puts great strain on police resources) to gather sufficient evidence to convict the organisers or backers of large scale drug dealings without recourse to interceptions.[10]

4.12 The Australian section of the International Commission of Jurists felt that the Stewart Royal Commission recommendations, rather than this Bill (Telecommunications Interception (Amendment) Bill 1986) are appropriate.

> It is sometimes absurd to restrict it. ...We believe, as does the New South Wales Bar Association, that the power ought to be there for serious crime, including drugs, but not just limited to drugs.[11]

4.13 Mr Richard Hall, author of Disorganised Crime, although in support of the extension believed that the power should be confined to drug offences and life threatening offences.[12]

4.14 It is the view of the Victorian Police Association that the Bill should not confine itself to offences relating to drugs and security.

> There are far more serious crimes committed against the community, such as murder, kidnapping, corruption, together with crimes caused by drug addiction but not linked directly to the drug chain, that is, armed robbery, extortion, the organised crime control enterprises, gambling, prostitution, labour manipulation on a large scale, tax and laundering of criminal proceeds.[13]

4.15 In 1983 the Australian Law Reform Commission (ALRC) stated in its Privacy Report that 'the third major criticism of the extension of interception powers to narcotics investigations is that there will be increasing demands to extend them further to other particular problem areas or even for law enforcement purposes generally. Looked at historically, there may well be valid justification for that apprehension.'[14]

4.16 Although the ALRC expressed some nervousness about supporting an extension in 1979, in evidence to this Committee the ALRC said:

> ALRC adheres to its recommendation that a warrant to intercept communications passing over a telecommunications service should be available in relation to all serious offences so defined. The present restriction to 'narcotics offences', and the restriction that would obtain upon the passage of the Bill to 'serious trafficking offences', cannot, it is suggested, be logically sustained.[15]

4.17 The AFP supported the extension of powers beyond 'serious trafficking offences' but in a stringently controlled environment. The Commissioner on request from the Committee developed five models which could possibly be used to legislate with respect to serious offences. He submitted however, that in developing the five models,

> ...I have maintained my stance that the preservation of one's right to an expectation of privacy when using the telecommunications system, is of primary importance and not to be lightly cast aside. In furtherance of my concern relative to the privacy issues my preferred model below would only be acceptable when operated in a stringently controlled environment.[16]

4.18 This sentiment was further supported by AFP officers, when in evidence to the Committee they stated:

> Where there is a high degree of sophistication or oganisation involved in criminal activity and where the principals are insulated by a variety of methods, obviously telephone interception could be applied in the same fashion as it is to narcotics.[17]

The Case Against the Extension of Powers to Serious Offences

4.19 Typical of the evidence given against the extension of powers to serious offences was that of the President, Australian Civil Liberties Union (ACLU). He said:

> The proposal to allow phone tapping in the investigation of non-drug crime is an example of the inevitability of the net widening effect of introducing even restricted powers.[18]

4.20 He went on to say:

> I think that the proposal to extend phone tapping powers is unnecessary, is a threat to privacy, is a threat to freedom of speech, has not been sufficiently justified and should be resisted. It should be resisted almost irrespective of the theoretic safeguards in relation to possible abuse of extended phone tapping powers ... it is unlikely to have any significant effect in curbing major crime.[19]

4.21 The witness for the New South Wales Council for Civil Liberties said, 'the Council was opposed to the extension of powers beyond 'narcotic drug offences':

> ...the Council's general approach is that lots of police generally seek wider powers to invade civil liberties in the name of opposing whatever crime is the crime of the day. At the moment it is drug crimes. Council says that these extended phone tapping powers are not justified .... We would certainly oppose widening the State powers[20]

4.22 The witness for the Law Society of New South Wales, said the Society was 'implacably opposed' to the extension of powers.[21]

4.23 He went on to say:

> There is no doubt that the power to intercept telephone conversations would provide police with additional intelligence, some of which could lead to the solving of crime. It is submitted, however, that the price to be paid in terms of democratic values, is too high a price ... It is not a question of 'how serious should the crime be, to allow phone tapping' but rather should be a matter of principle that phone tapping should be prohibited altogether.[22]

4.24 The Australian Telecommunications Employees Association (A.T.E.A.) stated in evidence to the Committee that:

> Clearly, underpinning our submission is an acknowledged aversion to a widening of phone tapping powers. The submission noted that this was founded on a broad philosophy which believes that the right to security and privacy is an essential feature of any democratic society. ... We believe that there is no good reason to extend phone tapping either beyond the one law enforcement agency, the Australian Federal Police, or beyond the one suspected offence, that of a suspected narcotics offence[23]

4.25 The Law Council of Australia saw much force in Justice Stewart's arguments for the extension. 'Nevertheless the extension of the warrant issuing power to cover serious trafficking offences is sufficient to meet current needs. Any widening of the power would require careful consideration for it would necessarily represent a further erosion of individual rights to privacy.'[24]

The Mechanism for Legislating with Respect to Serious Offences

4.26 An important aspect of the Committee's inquiry was to determine the most appropriate mechanism for legislating with respect to serious offences. This in turn required detailed

consideration of the term 'serious offence'. The Australian Law Reform Commission, in its 1983 Report, No 22, Privacy, defined 'serious offence' as:

> An offence punishable by imprisonment for life or for a term of not less than 7 years, whether or not the offence is also punishable by the imposition of a fine, but does not include an offence that is punishable by imprisonment for life or for a term of not less than 7 years by reason only that it is a second or subsequent offence.

4.27 Mr Justice Stewart's opinion was that:

> The difficult thing always in law enforcement matters, and indeed with legal matters generally, is where to draw the line. Whether you make it crimes that are punishable by seven years imprisonment or whether you do that some other way is always difficult .... I do not think you can just include everything over seven years or everything over five years or everything over 10 years. My view is that this should be left to the judicial officer to whom you apply for a warrant. That judicial officer should have certain guidelines, there cannot be carte blanche.[25]

4.28 The President of the Australian section of the International Commission of Jurists, suggested that:

> ...the legislature has usually made that decision for you. In every Act, you decide whether it is a summary offence or an indictable offence. ...but if you have to draw a line I think it should be drawn on matters that ultimately would go before a jury rather than before a magistrate. Even though there are many serious crimes before magistrates, they normally carry only two years' maximum penalty or fines of $1,000, $2,000 and so on.[26]

4.29 The Committee received many suggestions about how to define a 'serious offence' and the means by which 'serious offences' could be incorporated in the Act. These included propositions that:

a. rather than producing an extensive list of specified offences it would be more sensible to specify offences which carry terms of imprisonment over a certain number of years. Serious offences should be defined according to the number of years of maximum or minimum sentence that can be imposed under criminal statutes;[27]

b. the applicable serious offences be specified in a list which would form part of the Act;

c. there be judicial discretion to evaluate offences in terms of:

(1) the gravity of the matters being investigated

(2) the extent to which the privacy of any person is likely to be interfered with, and

(3) the extent to which the prevention or detection of the crime in question is likely to be assisted by the interception, and

d. all serious offences be defined as indictable offences, therefore not including summary offences.

4.30 The Committee also gave detailed consideration to the five models or mechanisms developed by the AFP. Their first model was to simply adopt a penalty criterion for offences which attract a maximum penalty of not less than seven years

imprisonment. The AFP considered that the simplicity of this approach, while attractive, fails to address the seriousness of the specific offence committed or is likely to be committed.

4.31 The AFP's second model is a variation of the first. It still provides an initial prescribed penalty criterion but also has others attached, to take full account of the seriousness of the offence against which is balanced the right to an expectation of privacy. It will probably require a judge, prior to issuing a warrant, to be satisfied that the invasion of privacy likely to result from the issue of the warrant is justified, having taken into account such issues as the investigative methods used and results obtained, availability and likely success of other investigative methods, the circumstances of the offence (or offences) committed, or likely to be committed, including the magnitude of the offence and the gravity of the particular consequences of the offence (or offences). The AFP considered that this model when operated within a stringently managed system, should provide ample and effective safeguards in respect to the privacy issues without unduly hampering police investigation of serious offences. Further, the AFP considered that the model suffers from the fact that some offences carrying maximum penalties of less than whatever penalty is prescribed may, on occasion, have consequences out of all proportion to the provided maximum penalty, but would not be included.

4.32 The third model the AFP considered was essentially that of the second model with allowance made in relation to offences having a maximum penalty of less than the prescribed penalty. In the AFP's opinion the third model has all the safeguards of the second model while at the same time providing a carefully controlled method of obtaining authority to seek the issue of a warrant in exceptional cases not included in the basic criteria.

4.33 The fourth model would be to simply leave the issue of a warrant in relation to any offence entirely in the hands of a judge, requiring only that the judge consider issues of the nature as set out for model two; i.e. model two without the prescribed penalty criterion. The AFP does not support this approach as the use of a prescribed penalty criterion provides a significant safeguard in keeping with the Parliament's perception of the seriousness of an offence as measured by the maximum penalty attached thereto.

4.34 The fifth model which the AFP considered was that of specifying in legislation specific offences. This approach, in their opinion, although attractive at first, is cumbersome and probably would quickly be found to be wanting; serious offences not listed may occur, leading inevitably to renewed pressure for a further extension of the power to intercept telecommunications. The rigidity of this approach, coupled with the considerable workload associated with maintaining the currency and relevance of the legislation as offences are created and abolished, is such as to render it inadvisable.[28]

4.35 The AFP recommended the third model to the Committee 'as it maintains a high standard of legislative safeguards, and judicial scrutiny, while also providing the operational flexibility so essential in investigating the commission, or likely commission, of serious offences'.[29]

4.36 The majority of the Committee favoured defining in the legislation serious offences, for the following reason. A modified model 5 places responsibility with Parliament to determine the circumstances in which the privacy invasive technique of interception may be justified, enabling the Parliament to amend the Act in response to community demand. It does not delegate this power and it does not confer upon the judiciary a possibly compromising and non judicial function.

Conclusion

4.37 The Committee repeats the observation made in Chapter 3, that, somewhat surprisingly, little public interest was evident throughout the inquiry. The lack of a strong positive response from the State Governments made the Committee's task difficult. The most compelling argument for the extension of powers to intercept for serious offences was the frustration being experienced by law enforcement agencies in their fight against 'organised' crime. It was argued very strongly and persuasively that these agencies should be granted every possible investigatory tool to enable them to compete on the same technological level as 'organised crime' and gather an intelligence data base. The opposing arguments, were based on an inherent right to individual privacy.

4.38 The Committee debated at great length the fundamental principles espoused by both proponents and opponents. Law enforcers must have the ability to intercept the telecommunication system for serious offences which are arguably more destructive to society than 'serious trafficking offences'. At the same time, the privacy of communications and the integrity of the telecommunications system is paramount.

4.39 The Committee concludes therefore on balance that:

a. a case has been made for police to have ready access to intercepted information in only the most serious offences, as well as serious trafficking offences;

b. the number of serious offences for which intercepted information should be available should be kept to the absolute minimum;

c. serious offences should be defined in the Act;

d. if the incident and nature of offences gives rise to community concern that interception powers ought to be extended to cover further offences this should be reflected by a further amendment to the Act by Parliament; and

e. until Parliament otherwise provides serious offences defined in the Act should be restricted to only:

(i) murder,

(ii) kidnapping, and

(iii) organised crime associated with offences:

(a) that involve 2 or more offenders and substantial planning and organisation; and

(b) that involve, or are of a kind that ordinarily involve, the use of sophisticated methods and techniques; and

(c) that are committed, or are of a kind that are ordinarily committed, in conjunction with other offences of a like kind; and

(d) that involve kidnapping, murder or serious drug trafficking offences and associated financial dealings in each case,

or which relate to conspiracy to commit any of the above offences.

Endnotes

1. The Hon Mr Justice D.G. Stewart, Report - Volume One, Royal Commission of Inquiry into Alleged Telephone Interceptions, 30 April 1986, p354 (henceforth cited as Stewart, Report)
2. H.R. Deb. (4.6.86) pp4595-4596
3. Stewart, Report, p339
4. Stewart, Report p.343
5. The Hon Mr Justice D.G. Stewart, Report, Royal Commission of Inquiry into Drug Trafficking, February 1983, p.659 (henceforth cited as: Stewart, Report p659 Drug Trafficking)
6. Stewart, Report pp.340-341
7. Stewart, Report - Drug Trafficking, p.656
8. Stewart, Report p.343
9. Stewart, Report p.343
10. Evidence, p443
11. Evidence, pp549 and 551
12. Evidence, p849
13. Evidence, p205
14. Australian Law Reform Commission, Report No 22, Privacy, Volume 1, p357
15. Evidence, p866
16. Exhibit, Australian Federal Police, No. 3, p1
17. Evidence, p122
18. Evidence, p177
19. Evidence, p167 and 169
20. Evidence, pp812-813 and 817
21. Evidence, p1101
22. Evidence, p 1084 and 1086
23. Evidence, p 674 and 670
24. Submission, Law Council of Australia, No. 42, p24
25. Evidence, pp476-477
26. Evidence, p.551
27. Evidence, p.415 and p.205
28. Exhibit, AFP, No 3
29. Exhibit, AFP, No 3

CHAPTER 5

THE PROBLEM OF ILLEGAL INTERCEPTION

Introduction

5.1 In the final recommendation in his Report, Mr Justice Stewart urges that:

> It should be an offence to sell or advertise for sale electronic devices designed for effecting telephone interceptions. Such devices should be made prohibited imports.[1]

5.2 At first consideration, it may appear that the issue of illegal interception, and the ease of access to devices capable of effecting illegal interception, may be outside the scope of the Committee's terms of reference. However, as indicated in Chapter 1, the Committee accepts that the main philosophical intent of the Act is to prohibit interception. In the course of this inquiry, the Committee took evidence which indicated a degree of acceptance in the community that illegal interception is continuing on a large scale. In preparing its position on the Bill, therefore, the Committee felt it necessary to address this issue in its report to the Parliament. This Chapter serves that purpose.

The Problem Defined

5.3 In evidence to the Committee, witnesses from Telecom Australia advised that, in the 12 months prior to September 1986, Telecom had become aware of 18 incidents in which devices were attached to telephone services for unauthorised purposes.[2] But they further admitted that these were only the incidents which

had come to their attention, saying that '[t]here is no organisation within Telecom that goes around exclusively checking for improper accesses or for improper connections to the network'.[3]

5.4 In response to a question taken on notice, Telecom subsequently provided the following table of illegal devices which had come to Telecom's attention since 1982-83:[4]

Table 5.1

NUMBER OF DEVICES LOCATED (BY YEAR)

	NSW	VIC	QLD	W.A.	S.A.	TAS	TOTAL
1982-83	3	-	-	1	1	-	5
1983-84	5	-	2	1	-	-	8
1984-85	2	1	1	1	-	-	5
1985-86	2	3	7	1	2	1	16
					TOTAL		34

5.5 Of these 34 incidents, Telecom advised that there has, to date, been only one successful prosecution under the Act. Moreover, these figures must be quite considerably qualified, because Telecom does not know, and has no way of discovering, the extent of illegal interception being undertaken across Australia. As Telecom's chief security officer, Mr W.F. Jamieson, put it to the Committee:

> ... the extent to which this illegal activity is going on is something which we really do not know. We only respond to those incidents that we become aware of in one way or another.[5]

5.6 The Director-General of Security, Mr A.K. Wrigley, advised the Committee that one of ASIO's functions was to provide protective security advice to Commonwealth departments, and that, as part of that process, ASIO could, to some extent, detect illegal interceptions. This, also, was qualified with the observation that '[o]ur knowledge of illegal telephone intercepts is limited to simply what might come out as a by-product of protective security advice to government departments and ministerial offices'.[6] Mr Wrigley further advised that, to his knowledge, no illegal devices had been found by ASIO personnel in their occasional security surveys of Ministers' offices etc. 'Aberrations' were occasionally found, suggesting possible tampering, and these were reported to Telecom.

5.7 A key piece of evidence followed, in response to successive questions. Asked firstly whether equipment capable of effecting interceptions should be limited in their public availability, Mr Wrigley said that:

> As a theoretical concept, I would agree. As a practical one, I doubt whether you could. A telephone is a pretty basic piece of machinery and it is not at all difficult for someone with the will to intercept it. I do not believe you could particularly effectively prohibit it by any sort of legislation. I think people will find a way quite readily of intercepting a telephone if they wish to do so.[7]

5.8 Mr Wrigley further stated that:

> ... people who have any cause to wish to have confidentiality about their telephone conversations and who have some public prominence, or commercial prominence for that matter, should, I think, assume that if someone wishes to tap their telephone he will find a way of doing it.[8]

5.9 In subsequent evidence to the Committee, Telecom's Chief Security Officer agreed that the detection and apprehension record for illegal interceptions was not good. But this state of affairs was compounded by the free availability to the public of induction and other devices capable of intercepting telephone conversations - 'there is very little control on the distribution, advertising, sale or availability of things like this. So the practice of illegally recording a conversation is made easier by that availability'.[9] Mr Jamieson referred the Committee to his earlier exposition of Telecom's position on this matter, saying that Telecom would strongly support the introduction of legislation prohibiting the sale or possession of devices capable of illegal interception:

> We have a strong view about the extent to which devices which may assist illegal interception are currently publicly easily available in this country. I think our view goes to the point of suggesting that it would be helpful for the legislators to look at the question of adopting legislation similar to that which applies in other countries, where it is not just the operation or the attachment of these devices which consititutes an offence, but where the actual import, advertising, possession, or the sending through the mails of these things constitutes an offence.[10]

5.10 The Committee had difficulty in obtaining reliable and accurate evidence, in public, on the extent to which the free availability of interception devices has contributed to widespread and continuing illegal interceptions. But a range of witnesses, across widely differing political persuasions and with fundamentally differing moral and ethical positions on the questions posed by an extension of interception powers, tended to confirm an impression of large scale abuse of the current interception law. A cross-section of anecdotal evidence is in the following paragraphs.

5.11 Mr Richard Hall, journalist, author of Greed, The Secret State and Disorganised Crime, told the Committee that:

a. if you are to believe even a fraction of what you are told, the scale of private bugging in this country is very large;[11]

b. Either all these anecdotes are wild exaggerations - you have to be cautious, but we see it in politics, we see it in crime, we see it in other people - or alternatively there is some fire in all that smoke out there. If so, it is quite a serious question.[12]

c. Let us just concentrate on, say, your heroin exercise, those big wholesalers who are making more money than criminals have ever made before. Of course they are using electronic devices. The police have had the problems which they must have talked to you about, about the scanners on police cars, detection devices on bugs for trailing. The police complained to me that ASIO was able to afford to install in all its cars devices which stopped scanners working on them, but the police were unable to. Your big criminal, your big heroin wholesaler - again it would be invidious to mention names - are underemployed to an extent. They have an awful lot of money and toys to play with. Certainly one who was operating in Sydney was an absolute self-taught electronic whiz-kid fanatic. The resources are unlimited in the sense that they can set $1m aside to perfect their operation. I will not say any more about that; it might be sailing too close to the wind. But if you have a cashflow, you can buy the best toy, any device.[13]

5.12 In oral evidence to the Committee in support of the National Crime Authority's submission, Mr Justice Stewart made it quite clear that the recommendation in his Report was, in his view, still valid, and that prohibition was, by definition, a practicable thing:

> I believe that the Government does have a responsibility ... to make it illegal to sell and import devices of this nature ... It is never too late, in my view, no matter how close to midnight it might be.[14]

5.13 This position was also put strongly in the NCA's submission:

> ... the Authority urges closer attention to illegal intercepts and the level of penalties attaching to them. Interception devices are still freely available and advertised in Australia, so it is highly likely that their use in industrial espionage and for other purposes by criminal elements is widespread.[15]

5.14 Mr Justice Stewart's stance on this issue was endorsed by various civil liberties groups which appeared before the Committee. Mr John Bennett, President of the Australian Civil Liberties Union, referred in evidence to the claim in Mr Justice Stewart's Report that more than 30,000 potential interception devices were sold in the year to March 1985. He said that there was a 'need for greater control of the sale of such devices. There is a problem with more and more technology becoming available to potential snoopers, to police agencies and to members of the public'.[16] He went on to cite a recent claim by a senior executive of a corporate security company in Sydney that:

> ... 11 companies in Sydney employ Webster to check their offices for bugging devices on a regular basis ... fitting a bug is relatively simple. It can be done by anybody disguised as a window cleaner, Telecom engineer or even a plant waterer. You do not even have to enter the office. Phones can be tapped simply by tampering with Telecom equipment in office basements.[17]

The Stewart Royal Commission: Interception Equipment

5.15 From information gathered by investigators working with Mr Justice Stewart, the most common device sold by retailers in Sydney, for as little as $2.25, is the telephone induction coil. The device 'consists of a suction cap which is affixed to the handpiece of a telephone and connected to a tape recorder by means of a plug'.[18] Another device highlighted in the Report was the VR200 voice reactor, sold as a telephone accessory. This is wired into the telephone circuitry and connected to a tape recorder which is set on the record mode. The tape recorder is activated when the handset is lifted. According to Stewart, this device retails for about $10.00.[19]

5.16 Other devices cited in the Report include:

a. a basic transmitter fitted with wires which can be clipped on to a telephone line at a terminal;

b. an FM wireless microphone retailing from about $25.00, which can be adapted to intercept telephone conversation, and is stocked by most retailers of electronic devices;

c. a cheaper version of the FM wireless microphone called the 'Fun Bug' retails for $9.95; (According to the Report, this device has been taken off the market by two large retailers due to its potential illegal use.)

d. an electronics kit designed as a child's toy, which has the capability to intercept calls;

e. a sophisticated device which retails for approximately $1,000. The device consists of a transmitter fitted with wires which can be

connected to the telephone lines, but appears to be only imported on a 'firm order' basis (it is available from at least two Sydney retailers), and

f. portable scanners retailing from $160.00 - $430.00.

5.17 Mr Justice Stewart also referred to widespread advertising in Sydney of the devices which have been described in the preceding paragraphs. The advertising is in the form of trade and other magazines and catalogues. They are readily accessible to the general public. The literature describes the product range which includes devices and gives details of the manufacturer, wholesaler and/or retailer. The instruction manuals for the devices are also available from the distributor.[20] The range and widespread availability of devices is illustrated in the extract from a catalogue copied as Annex A to this Chapter. The catalogue was provided to the Committee as part of Telecom's submission. It is entitled 'Alert '86', and is from the Australian Security, Fire and Safety Trade Fair. It provides a detailed description of the types of interception devices available and the names, addresses and services offered by various electronics and security companies.

Commercial and Industrial Espionage

5.18 It is not only the illegal interception of voice transmissions over a telecommunications system which is covered by the Act and the Bill. Also of concern to the Committee is the extent to which the telecommunications system may be used to intercept illegally the increasing range of non-verbal transmissions, some of high commercial or personal sensitivity, being effected through, for example, telex, facsimile, digital transfer. The Committee sought confirmation from the Attorney-General's Department that the principal Act, and therefore the Bill, apply to non-verbal communications. The advice was unequivocal:

> This Department has consistently advised that 'communication passing over a Telecommunications system' is not limited to speech. Any communication, that is any transmission of information or of a signal comes within the *meaning of 'communication'*. Accordingly, non-verbal means of transmitting information over telecommunications systems operated by the Australian Telecommunications Commission are covered by the provisions relating to interception contained in the Act.[21]

5.19 The issue of illegal interception being used to effect industrial espionage was covered briefly in Justice Stewart's Report:

> The Commission is aware that industrial espionage in relation to telephone services is not limited to the interception of conversations between persons. Telephone lines are also used to transmit messages from computers. These can be intercepted using an FM transmitter and and FM radio receiver. By using a computer 'modum' with printer attached, the message can then be converted to print. These devices are readily available from retail outlets.[22]

5.20 The Committee did not have the capacity within the available time to pursue this matter with any thoroughness. It notes with concern, however, that the free availability of devices capable of effecting interception must inevitably compound a steadily increasing problem.

5.21 In an attempt to make a preliminary judgement of the extent to which a major problem does in fact exist, the Committee took in-camera evidence from witnesses whom the Committee knew to be both appropriate and reliable. Hearings were held in-camera at the request of the witnesses, in order not to jeopardise legitimate commercial concerns. The Committee agreed to the hearings on that basis, respecting the wishes of the witnesses. The evidence was startling, as demonstrated by the following extracts:

a. I have no idea how many telephones are being intercepted on a daily or weekly basis. I can only suspect, from the information that I have been given by the people that we deal with [police, law enforcement and other government agencies], that the number is much higher than we suspect.

b. ... there was a group of people in Sydney who were - this is my term, 'casual intercept operations' - placing devices on spec, obtaining information and then offering that information for sale.

c. ... from what they have knowledge of and what they are finding on a daily basis is going on, it must be much greater than any of them would anticipate.

d. I honestly believe it [banning the sale of intercept devices] would have no effect at all because, essentially, those people who would break the law by using their own devices would still continue to break the law. Certainly you could outlaw the sale, possession or what have you of telephone intercept devices, but a pair of crocodile clips and a set of headphones is a telephone intercept device; a tape recorder with a set of crocodile clips is a telephone intercept device. It is the act of interception itself which, I understand, is illegal now except in specific cases. I think it would discourage those people perhaps who may be thinking about it from doing it, but certainly at a higher level, no.

5.22 Other technical evidence caused the Committee some disquiet and confidential copies of this evidence have been forwarded to the Attorney-General and the Special Minister of State for their information.

Conclusions

5.23 At the outset, it should be stated that the Committee accepts that a total ban on the importation, distribution, advertising and sale of devices capable of effecting interceptions will not stop illegal interceptions. For those determined to do so, ways and means will always be found, ranging from the placing of a simple 'crocodile-clip interception' to the surreptitious importation of sophisticated scrambling, recording and interception electronic devices.

5.24 This being the case, it may well be argued by some that an importation and sale ban would be futile, in that it can never achieve the desired effect of halting illegal interceptions. The Committee does not accept this proposition. It supports the underlying thrust and intent of the Telecommunications (Interception) Act 1979, which is to prohibit interception except under few and carefully defined circumstances. It mocks the law to prohibit an activity but permit the open encouragement of that same activity through commercial sale and public availability.

5.25 Accordingly, the Committe concludes that:

a. the extent of illegal interception would be lessened if the availability of devices designed solely for telecommunications interception purposes was substantially reduced;

b. widespread advertising of potential interception devices encourages a disregard for the law;

c. the range of illegal interceptions must be reduced;

d. devices designed solely for effecting interceptions should be declared prohibited imports, subject to control by Government licence for specific law enforcement purposes;

e. the manufacture, importation, advertising, sale and possession of such devices should be made illegal, and subject to penalties in accordance with those prescribed for physically effecting interceptions, and

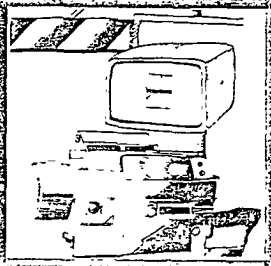
f. Telecom should actively pursue the maintenance of the integrity of the network and the detection of illegal devices as a matter of urgency.

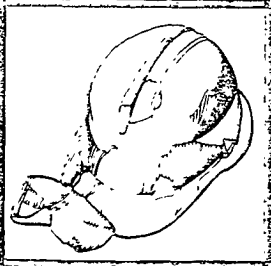
Endnotes

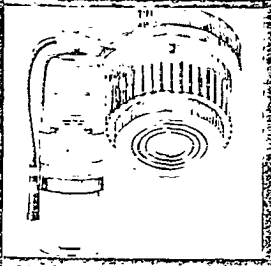
1. Stewart, Report, p356
2. Evidence, p274
3. Evidence, p291
4. Submission, No 35, Telecom Australia, p10
5. Evidence, p292
6. Evidence, p348
7. Evidence, p353
8. Evidence, p353
9. Evidence, p606
10. Evidence, p292
11. Evidence, p853
12. Evidence, p856
13. Evidence, pp856-857
14. Evidence, p491
15. Evidence, p447
16. Evidence, p180
17. Evidence, p182
18. Stewart, Report, 243
19. Stewart, Report, 243-244
20. Stewart, Report, 246-247
21. Letter to the Committee Secretary from the Attorney-General's Department dated 16 September 1986
22. Stewart, Report, 249

THE Exhibition Company...

AUSTRALIA 86



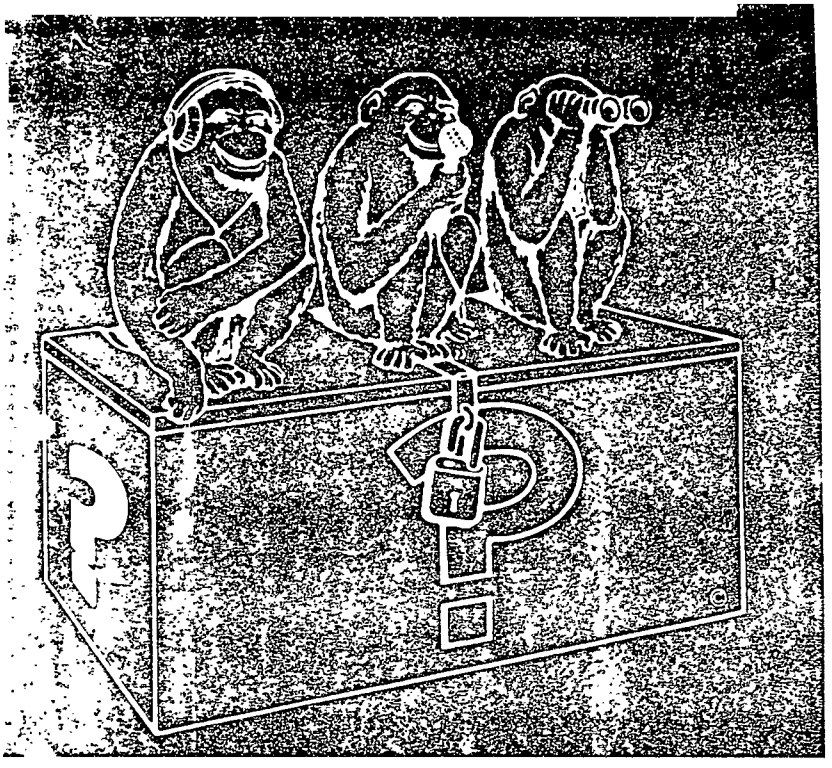




THE AUSTRALIAN SECURITY FIRE & SAFETY TRADE FAIR

CATALOGUE

R.A.S. SHOWGROUND SYDNEY
TUESDAY AUGUST 5 — 10.00AM-6.00PM
WEDNESDAY 6 — 10.00AM-8.00PM
THURSDAY 7 — 10.00AM-6.00PM



fort knox

ELECTRONICS SECURITY

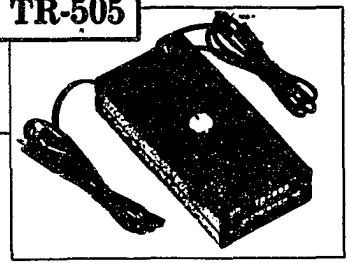
29 GLENGALA DRIVE ROCHEDALE 4123 QUEENSLAND AUSTRALIA
TELEPHONE (07) 341 6513 TELEX AA 40472 PUBTLX BR670

Auto Telecorder

For Perfect and Automatic Recording of Telephone Conversation

When connected to your tape-recorder, the tape runs only when a conversation goes on. Thus you can avoid waste of tapes.

TR-505



Crystal-Controlled Tapping System with Wireless Microphone

CX-07 is a combination set of transmitter and receiver, both of which are crystal-controlled. It tappes with a far better wireless microphone than the one through an ordinary FM radio.

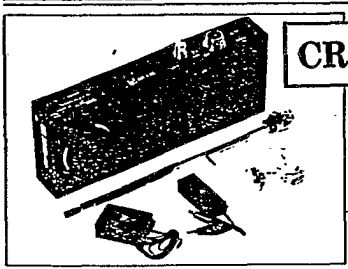
Features of CX-07

1. Frequency adjustment unnecessary: The frequency is pre-set by crystal, so you just push the button to listen to the conversation.
2. Superior mini-size: Both the transmitter and the receiver are designed for the maximum efficiency in the minimum size. Especially the receiver can be put inside the breast pocket of your shirts.
3. Special frequency: The extremely specific frequency prevents you from being tapped by a third party.
4. 2-channel system: You can hear two conversations simultaneously by installing the transmitter at each place.
5. High quality: Clear and vivid voice sound reaches you 'far' from 700 meters under non-obstacle wave path. No other wireless microphones can do this.
6. Easy recording: By connecting a recorder to the receiver, you can easily listen to a conversation through the earphone while being recorded.
   (size of tape-jack: 3.5)

CX-07

CX-01 1 Channel Type

CZ-10 Handmade for Pros (2 Channel)

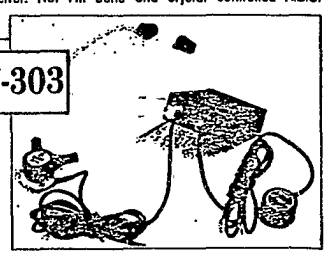


CR-120

Carrier Controlled Auto Tape Recorder

The Cr-120 is precision technology and a superb piece of professional equipment. It will automatically record when it is activated by the target telephone TX-5 Transmitter and re-layed to NCZ-10 Receiver. Not FM band and crystal controlled A.B.C. channels.

MW-303



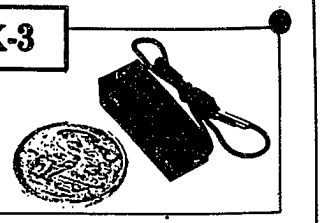
Concrete Mike

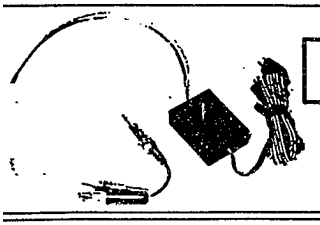
You can listen to a conversation beyond a thick concrete wall or in the next room clearly. A combination of the most modern electronic technology and acoustic oscillatory engineering has given birth to this epoch-making "Wall Microphone". Unlike other acoustic amplifers, it turns oscillations transferred to the wall into voice waves. **It certainly deserves to be called a "real wall microphone for professional use."**

ephone-Mitter Surveillance

power source needed. Automatic in operation. Transmits on F.M. nd. Can be installed indoors or outside. When installed properly most un-detectable Covers all branch lines from the line that it on.

TX-3





TS-401

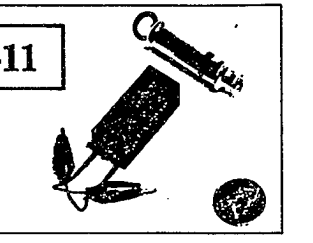
"Telephone Secretary"

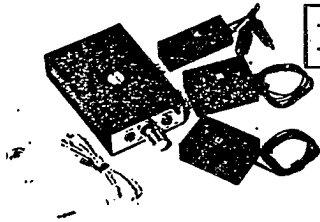
Brand New! Your Skilled and Dependable Secretary - A Telephone Conversation Recorder directly connected anywhere to the telephone. Simple. Inexpensive. Can be used with a tape recorder of any kind.

el ar"

Tele-Ear remotely monitors all sounds and voices at any n where there is a telephone nearby. The TE-11's unique uitry utilizes the existing telephone system, with very little lification, so that it can be controlled from, and transmits rmation to, the telephone which you are calling from **no matter ere in the world you happen to be.** For this reason the TE-11 is known as the "infinity transmitter". After installation, you can en at anytime and from anywhere with no fear of detection.

TE-11





NCZ-10

Crystal-Controlled Transmitter with Receiver

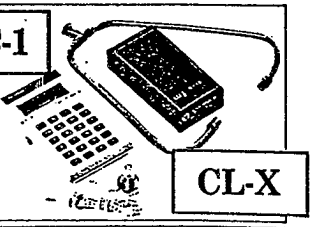
Surveillance crystal controlled special receiver remotely monitors sounds and voices in the room where the NCZ-10 special transmitter is located. High Tech quality and not to be confused with cheaper devices, this unit is crystal clear, ranged to 700 meters under non-obstacle path, three channel operation. Allows easy recording and utilised high performance earphones.

ireless Microphone of Hand-Held Electronic alculator

nsitive wireless microphone is installed inside the hand-held tronic calculator. No one can notice it from the outside. -1 can be of course used as an ordinary electronic calculator.

is a combination of transmitter and receiver, both of which are tal controlled. It is better in quality and easier to handle than -1.

CLC-1

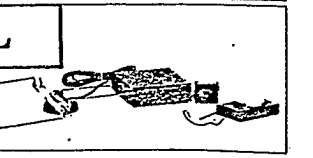


CL-X

ar Hunter — Electronic Car Tracer

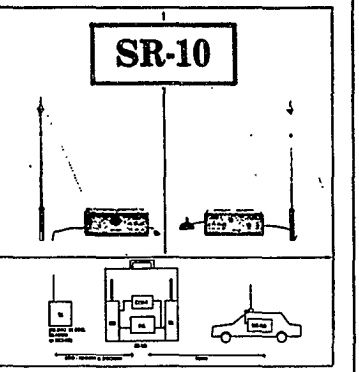
car hunter has been designed specifically for the needs of essional investigators. Completely transportable and easily rried to elevated locations. Ideal for use in urban as well as urban areas. Three channels. Continuous operation for 45 urs. Precise monitoring by tone beeps and LED indication. nge to 15km also Directional.

CL



SPECIFICATION MODEL
One Step Repeater

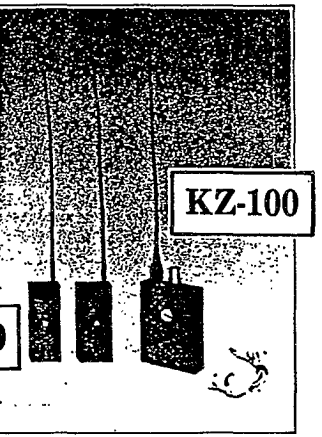
1. Receiver Freq. : 2 channels in 130-135MHz. Zone.
2. Transmitter Freq. : 1 channel in 144-148MHz. Zone.
3. Out Put Power : 10K/5K Changeable.
4. Power Supply : AC 220V. (with AC Cord)
   DC 12-14V. (with Car-Batt. Cord)
5. Control System : Carrier control system:
   Receiver: Automatic start by receiving the carrier input from TX. and stop by input off.
6. Antenna : Helical Antenna for RX and TX.
7. Outer Case : Attache 436 × 310 × 80mm.
8. System Composition: 1 Transmitter (TX-200, TX-500 or TX-1000)
   1 Repeater (SR-10)
   1 Receiver (MZ-80 with Base & Antenna)



UHF MONITOR SERIES
nallsized UHF Transmitter

Although the output power is rather low, the reception area is considerable, extending about 600 - 800m thanks to the high sensitivity Receiver Model KZ-100.
If using 'Yagi' Antenna, the distance will be extend to 2-times.

Antenna : /4 Flexible.
Battery : Rithuim CR-2N×1 (3V) or UM5 × 2(3V).
Batt. Life : 130-140Hrs. continuously.
Dimension : 66 × 27 × 14mm.
Weight : 52gr. (68gr = with Batt.)
Frequency : One channel within 400-450MHz. bandwidth.
(Matching to Receiver).



Smallest and Hi-Sensitivity UHF Receiver

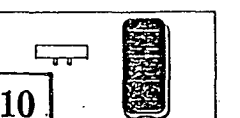
The monitoring sensitivity is very high There is no interception by other frequency due to the operation by very few noise and interference freq bandwidth.

Antenna : /4 whip Flexible.
Antenna Connector : RCA type.
Receiv. Channel : 2-channel "A" & "B" switchable.
Direction Antenna : "Yagi"
Dimension : 67 × 50 × 20mm.
Weight : 84gr. (94gr. = with Batt.)
Battery : Rithuim 2CR-1/3N (6V).
Battery Life : 30 Hrs. continuously.

Socket Type AC Transmitter

This AZ-110 fulfils its function by limitless AC power.
Once plugged in to AC power source it keeps on transmitting the sounds in the room covering a range of about 15m unless unplugged.
This AZ-110 has 3-outlets which can be used normally with 3 appliances . (Radio, Lamp or Clock).
As the output power is rather low, there is no interference for TV or other home electrical goods.

Power Source : 240V.
Service Area : About 800M using KZ-100.
If using "Yagi" antenna, the area will extend to 1.5km
Frequency : 1-channel within 400-450MHz.
(Matching Receiver KZ-100)



Electra-Cables (Aust) Pty. Ltd.
Cnr River Road West and Arthur Street, Parramatta, NSW, 2150.
P.O. Box 126, Parramatta, 2150
Telephone: (02) 635 7777
Personnel: Alex Duwakin, Susan Mitchell, Keith Hills, Glenyce Steadman.
Products: Electrical cables for security installations and security equipment.

Stand No. 47

Elkron Security
46 Monro Avenue, Kirrawee, NSW, 2232.
P.O. Box 261, Engadine, NSW, 2233.
Telephone: (02) 521 4222
Personnel: Richard Webster, Ron Waddell, Terry Vincent, Christine Vincent, Anne-Maree Robson, Sharon Wiltshire.
Products: Medium to high security detection equipment.

Stand No. 33

Esgard Australia Pty. Ltd. (Zannaeus Pty. Ltd.)
P.O. Box 278, Mona Vale, NSW, 2103.
Telephone: (02) 99 2787 (07) 375 5622
Personnel: Zachaeus Waldeback, Ulf Hertquist.
Products Ingstrom Escape Chute.

Stand No. 49

Express Alarm Supplies Pty. Ltd.
465 Pacific Highway, Artarmon, NSW. 2064
P.O. Box 558, Lane Cove, NSW, 2066.
Telephone: (02) 427 1233
Personnel: Michael Strong, Rob Colsell.
Products: Hirsch access control systems, Visonic passive infra-red detectors, Digit Alarm 908 digital communicator.

Stand No. 6

Focal Communications
123 Clarence Street, Sydney, NSW, 2000.
Telephone: (02) 290 1499
Personnel: Glenn Feldwick, Laura Rattos, Rachael Smithies.
Products: A wide range of training films and videos covering such areas as industrial safety, commercial and retail security, and fire prevention. All available training programmes will be screening at our stand throughout the exhibition.

Stand No. 82

Fort Knox Electronics Security
29 Glengala Drive, Rochedale, Qld. 4123.
Telephone: (07) 341 6513.
Personnel: Allen Knox.
Products: For details see Kenobi Cybernetics entry.

Stand No. 13 See Brochure

F.R.B. Industries Pty. Ltd.
7 Farr Street, Marrickville, NSW, 2204.
Telephone: (02) 569 6644
Personnel: Frank Burns, Ben Pender.
Products: Automatic doors, call points, security systems.

Stand No. 24

GEC Video Systems
2 Giffnock Avenue, North Ryde, NSW, 2113
P.O.Box 143, North Ryde, NSW, 2113.
Telephone: (02) 887 6222
Personnel: Ken Willoughby, Michael Andrews, Lindsay Fietz, James Goh, Dean Mills, Ted Johnes, Malcolm McGill, Paul Allanson, Neil Stewart.
Products: National range CCTV cameras, monitors and time lapse V.T.R.s, including the new CCD miniature camera and CCD colour video system, EEV thermal imaging camera.

Stand No. 36

Hadfield Sign Co. Pty. Ltd.
35 Gow Street, Padstow, NSW, 2211.
P.O.Box 443, Bankstown, NSW, 2200.
Telephone: (02) 707 4222
Personnel: John Hadfield, Terry London, Julie Hadfield.
Products: A full range of safety signage including specialised "low cost" fluted plastic signs, particularly designed for the building and construction industry.

Stand No. 85

I.E.I. (Aust) Pty. Ltd.
248 Johnston Street, Annandale, NSW, 2038
Telephone: (02) 692 0999
Personnel: Adrian Maidment, Ross Messina, Peter Lang, Michael King, Brian Davies.
Products: E700 VESDA (Very early smoke detection apparatus), E6800 Direct Line High Security System, range of microprocessor security systems for commercial, industrial and domestic applications.

Stand No. 32

Imperial Alarm Screens Aust. Pty. Ltd.
196-198 Railway Parade, Kogarah, NSW, 2217.
Telephone: (02) 588 6573
Personnel: Fred Cavanagh, Mark Cavanagh, Brett Cavanagh, Phillip Cavanagh, Mrs Cavanagh, Dennis Sales.
Products: A perimeter alarm system and special installing equipment.

Stand No. 16

Insurance Council of Australia
20 Bridge Street, Sydney, 2000.
Telephone: (02) 27 7761
Personnel: John Carmichael.
Products: Fire protection inspection services. Impartial reporting upon fire safety of all types of property including all relevant testing and inspection reuired in order to provide a true assessment of fire safety of a property.

Stand No. 102

International Security Electronics Pty. Ltd.
119 Cathedral St., Woolloomooloo, NSW, 2011.
Telephone: (02) 357 3266
Personnel: Bill Sheehan, David Barker.
Products: Range of security products including burglar alarms, control equipment, access control equipment, warning devices, car alarms, motion detectors, security lights.

Stand No. 40

Kenobi Cybernetics Pty. Ltd.
Unit 2, The Solander Centre, Solander Road,
King Langley, NSW, 2147.
Telephone: (02) 674 4533
Personnel: Ken Studdert, Kim Neat.
Products: Bug detectors, anti-surveillance devices, security electronic briefcase, telephone security unit, telephone scrambler, walk-through weapon detector.

Stand No. 13

Kimberly-Clark Australia Pty. Ltd.
20 Alfred Street, Milsons Point, NSW, 2061.
P.O.Box 343, Milsons Point, NSW, 2061.
Telephone: (02) 929 7133
Personnel: Robbie Stocks.
Products: Kleenguard non-woven overalls.

Stand No. 80

Knogo Australia Pty. Ltd.
431 Pacific Highway, Artarmon, NSW, 2064.
Telephone: (02) 428 1199
sonnel: Norm Dowsen, Craig McIntosh.
·roducts: Anti-shoplifting systems covering clothing and hard goods including liquor and books, sporting goods etc. Knogo has been in business for 20 years and we are the leaders in the anti-shoplifting systems industry.

Stand No. 30A

J. Larsen Pty. Ltd
383 St. Paul's Terrace, Fortitude Valley, Qld, 4006.
P.O.Box PMB 22, Fortitude Valley, Qld, 4006.
Telephone: (07) 854 1866
Personnel: J. Larsen, R.J. Larsen, J.C. Larsen.
Products: 'Viro' padlocks, 'Melsmetall' key control systems, 'Melsmetall' cash boxes and safes, 'Oz' security keying systems, 'Orion' key cutting machines and key blanks.

.d No. 14

Liftmaster Electronics Pty. Ltd.
241 Mitchell Road, Alexandria, NSW, 2015.
Telephone: (02) 519 2000 (02) 698 8000
Personnel: John Shaw.
Products: Electric latches, carpark access equipment, boom gates, shutter motors and swing and sliding gate operators.

Stand No. 11

Lord Safe Company
16 Ada Avenue, Brookvale, NSW, 2100.
Telephone: (02) 939 6888
Personnel: John Free, John Kelly.
Products: Security safes, fire proof record protection cabinets and files and computer data storage cabinets.

Stand No. 43

Luxolamps
9/98 Old Pittwater Road, Brookvale, NSW, 2100.
P.O.Box 717, Brookvale, NSW, 2100.
Telephone: (02) 939 2499
Personnel: Phil Dunn, Elizabeth Reyswoud, Pat Thompson, Jenny Monti, Elaine Elphick.
Products: Ergonomic products available are Helko ergonomic furniture, super holders or keyboard operator stands, VDU ergonomic arms and task lighting.

Stand No. 41

Martin Stoll Chairs
9/98 Old Pittwater Road, Brookvale, NSW, 2100.
P.O.Box 717, Brookvale, NSW, 2100.
Telephone: (02) 939 2499
Personnel: Eric Whiteley, Grant Whiteley, Brian Clarke.
Products: Ergo postural office seating.

Stand No.41

Medical Products (Aust) Pty. Ltd.
16 Newton Street, Auburn, NSW, 2146.
Telephone: (02) 647 2489 Telex 74352
Personnel: Steve Cramp, Laurence Mason.
Products: Medical safety and evacuation equipment e.g. Evac-chair, Jordon frame, Elsa emergency breathing apparatus, fire extinguishers and blankets, training aids.

Stand No. 57

Megoz Pty. Ltd.
35/47 Allingham Street, Condell Park, NSW, 2200
Telephone: (02) 707 2277.
Personnel: Geoffery Wall.
Products: Fire fighting equipment, fire detection equipment.

Stand No. 45

Metropolitan Security Services
27a South Street, Granville, NSW, 2142.
P.O. Box 407, Granville, NSW, 2142.
Telephone: (02) 682 4733
Personnel: Max Weeks, Brian Arnott, Peter Taylor, Mike Warren.
Products: Security alarm systems — Neva-Alone Personal Alarm, Mobile Security Patrol Services, Uniformed/Plain Clothes Guard Services, Security Document Destruction Services.

Stand No. 9

Mira Consultants Ltd.
7/50 Clarence Street, Sydney, NSW, 2000.
Tel: (02) 29 6223 (03) 614 5655 (09) 322 5477
Personnel: Stephen Sinclair, Jim Irish, Ron Thomas, Mike Nolan.
Products: Risk Management advisers, occupational health and safety, industrial hygiene, natural hazards, statistical and actuarial services.

Stand No. 73, 74

CHAPTER 6

ALTERNATIVES TO THE 1986 BILL

Introduction

6.1 Chapter 2 detailed some of the reactions to the Bill received in evidence by the Committee during its inquiry. The Committee has already concluded (see para 2.160) that the proposed legislation, the most recent of many amendments to the Act, compounds an already complex piece of legislation. As noted by a representative of the NSW Society of Labor Lawyers:

> The legislation consists of complex amendments to frequently amended, obscurely worded, legislation. If it is difficult for lawyers to make sense of the legislation then there is no prospect that non lawyers will understand it ... Whatever view is finally taken by the Joint Select Committee the form of the legislation itself raises important social issues. In short, and at a minimum, an entirely new Act should be drafted, in language that can be understood and debated by all concerned.[1]

6.2 In this Chapter, the Committee proceeds from the basis that the Bill in its present form is unsatisfactory in its premises and its drafting. It canvasses the merits of a new Act, and examines this possibility in terms of the coordination and implementation of interceptions each by one authority and the inclusion of essential safeguards, to include independent audit and scrutiny. The Chapter concludes by citing the limited evidence received in relation to financial considerations in extending telecommunications interception access.

A New Act?

6.3 At its first public hearing, the Committee sought to determine the policy with respect to circumstances where major amendment is proposed to an existing Act. A witness from the Attorney-General's Department told the Committee that it seemed that the Office of Parliamentary Counsel preferred to build on an existing framework of legislation, and to proceed by way of amendment. This was subsequently confirmed in writing by the Department:

> In the course of giving evidence before the Committee, the Committee asked why extensive amendments to the Act had been prepared, and whether consideration had been given to the preparation of a completely new Act. I am informed by the Office of Parliamentary Counsel that it is their policy, when changes are being made to an already existing Act, to deal with those changes by way of amendment.[2]

6.4 The Committee acknowledges the importance of precedent in the development and interpretation of the law. It also recognises the fine balance to be considered when deciding between re-drafting or legislating by amendment, particularly in highly sensitive areas such as telecommunications interception. The Committee also acknowledges the dangers involved in repealing legislation which may have been, as in this case, the subject of extensive judicial interpretation.

6.5 The Committee took pains during the inquiry to seek the considered judgments of practitioners of the law on the Bill and its effect on the Act. The spokesman on criminal law for the Law Society of New South Wales, Mr Trevor Nyman, told the Committee that, as a lawyer, he 'found it readable ... it was comprehensible to me'.[3]

6.6 Mr Nyman was the sole legal voice heard in evidence to speak favourably of the Bill. The weight of evidence was highly critical, and forms the basis for this Chapter's conclusion, on balance, that a new Act is necessary. A brief survey of other evidence put to the Committee is in the following paragraphs.

6.7 The Victorian Bar observed in its submission to the Committee that:

> the form of the amendments is extremely complex and will inevitably give rise to difficulties in interpretation. Particularly when an Act is to be amended in a substantial way, as in the case of this Bill, we consider it would be much more convenient and meaningful if the amendments were included within the Act reprinted in such a manner as to show what was the old Act and what was the amendment. The task of perusing the amendment Bill in conjunction with the old Act is a difficult one ... The drafting of this particular Bill appears to us to create enormous difficulties in sorting out not only how things fit together but what is actually intended.[4]

6.8 The Director of Research of the Australian Law Reform Commission explicitly added to the range of criticism of the Bill and its effect on an already complex Act. An ex-legislative draftsman, he told the Committee that he 'found the amending Bill difficult to follow ... It is typical of Commonwealth laws which are trying to deal with about 56 different things at once'.[5] He went on to outline to the Committee his views on the time it would take to re-draft this legislation in simple, un-convoluted language. If, following instructions, there was no requirement for lengthy conferences involving referrals back to contributing Departments, he thought a complete re-draft could be done within 10 days or so.[6]

6.9 It was put to the Committee by the Australian Law Reform Commission that the Commonwealth should consider 'the

issue of telephone tapping in the wider context of interferences with communications generally. These include oral communications and communications by mail'.[7] This was one of several suggestions to the Committee that surveillance law generally should be addressed in legislation. As the Commission observed in its 1983 report, Privacy:

> New technology has greatly increased the possibilities for secret surveillance. Listening and optical devices now enable intrusion into private activities previously considered unreachable. The capacity for communication, particularly telecommunications, has expanded, but so has the ability to intercept communications and to obtain private information. At the same time, the tradition of respect for communications carried by the post and telecommunications systems has been eroded by legislation and practices that pursue social objectives other than the protection of privacy.[8]

6.10 The Australian Law Reform Commission concluded, by majority, that, constitutionally, the Commonwealth could not legislate to incorporate the use of devices not physically connected to a telephone, but placed on or near one. The witness from the Commission suggested to the Committee that:

> you can provide that you will not authorise State officers to tap or to apply for taps, unless the State has laws satisfactory to yourselves concerning interception and communications over which there is no Commonwealth constitutional power. So control over ordinary listening devices, little pocket microphones and so forth, long range cameras, those sorts of things, the kinds of things which were dealt with by the Commission in its report, could be required of States as a condition of their having access to the telephone tapping facility.[9]

6.11 The Committee does not endorse this approach, which would not serve the wider interests of co-operative federalism. However, during its inquiry, the Committee noted with concern

some incidental evidence of the inadequacy of various privacy safeguards in State laws covering aspects of surveillance. The inadequacy of legal safeguards was amply demonstrated in a judgement in the Supreme Court of Queensland delivered on 17 September 1986, concerning which the Queensland Law Society made a submission to the Committee (No. 3507 of 1986, Mr Justice Dowsett: Robin Howard Reichelt, plaintiff, v. Sir Terrence Murray Lewis, Commissioner of Police). The case involved a solicitor who took action against the Commissioner of Police when an interview he had had with a client was monitored by police, recorded, transcribed and delivered to prosecuting authorities. Police asserted their right to do so under the Invasion of Privacy Act 1971-1976, Queensland. Mr Justice Dowsett's response was scathing. He described the police conduct as 'reprehensible', and made the following pertinent observation:

> There has been much public debate in recent years about the relative merits of traditional safeguards of individual rights on the one hand and statutory safeguards on the other. Our legal system depends both upon traditional, unwritten safeguards and statutory safeguards. So long as the community generally and the institutions of the State in particular recognise the unwritten safeguards and observe them faithfully, there is no reason to reduce those safeguards to statutory form. However, when traditional safeguards are attacked, as has happened there, it becomes necessary to consider the question of incorporating those safeguards into legislation...In facilitating the performance of their duties, confidentiality of communication between solicitor and client is critical. If police officers set themselves above that principle, then parliament may have to legislate to enshrine the principle in our law.[10]

6.12 The Queensland Law Society submitted that this judgement was relevant to the Committee's inquiry on the following grounds:

a. authority to intercept conversations is often granted secretly, without any subsequent public scrutiny - 'in the heat of an investigation relating to a serious offence police officers involved may cease to exercise dispassionate judgment and may abuse the benefit of a judicial approval ... the procedure for obtaining the order should be as painstaking as possible';[11]

b. warrants should identify telephone services to be intercepted and be strictly limited by time, creating an effective judicial audit, and

c. 'no procedure should be created which may permit the interception of conversations between a legal practitioner and his client ... to remove the right to independent legal advice ... is to remove a cornerstone of the administration of justice'.[12]

6.13 The Committee believes that interception law as well as surveillance law generally must be based on respect for the rights of individual privacy and the prevention of abuse of interception powers. There must be, as the Law Council of Australia submitted, 'explicit procedural protection for the evident legislative presumption favouring privacy of the individual'.[13] The subject Bill fails among other things to incorporate in the Act proposals for judicial consideration, in the granting of warrants, of the gravity of matters being investigated and of the extent of privacy invasion.

6.14 It is outside the scope of this Committee's terms of reference to canvass fully the areas into which federal legislation covering aspects of surveillance might go. On the basis that the Committee concludes that the Telecommunication (Interception) Act 1979 is inadequate, the Committee recommends that re-drafted legislation should take in the broader issues of privacy rights in the context of all surveillance devices for which the Commonwealth has the constitutional power to legislate.

6.15 The Commonwealth has un-fettered power, for example, to legislate to cover listening devices in the Australian Capital Territory. It has not done so. The Commonwealth's power under section 51(v) of the Constitution includes power over broadcasting. It appears to the Committee, therefore, that the Commonwealth could consider legislating, to the extent of its powers, with respect to listening devices which operate through broadcasting.

6.16 The present mixture of differing Commonwealth and State legislation in this field causes the Committee some concern. The situtation was summarised in the Australian Law Reform Commission's 1983 report, Privacy, as follows:

> Commonwealth legislation regulates the use of listening devices in matters related to national security and the investigation of narcotics offences only. State legislation regulates listening devices otherwise. There is no such legislation in Tasmania, the ACT or the Northern Territory. The laws of the mainland States are by no means consistent in their approach. They do not apply to Commonwealth officers using listening devices in the course of their duty, or, at best, their application is a matter of considerable doubt and obscurity.[14]

6.17 The Committee makes the recommendation, incidental to its terms of reference, that the Commonwealth Government move to introduce legislation defining and, where necessary, restricting, the use of listening devices, to the extent of its power under the Constitution. Given that some States have already moved to effect legislation in this area, the Committee further recommends that uniformity of safeguards and procedures should be the aim.

6.18 The Committee strongly recommends that the Commonwealth proclaim a model code for the use of listening devices in the Australian Capital Territory, and use what influence it enjoys to encourage uniformity of standards between the States.

6.19 The Committee recommends, in summary, that:

a. the subject Bill be withdrawn;

b. there be substituted for the subject Bill a Bill for an Act to consolidate and re-structure the principal Act, incorporating the applicable provisions of the subject Bill and the recommendations contained in this report;

c. the Commonwealth, through enacting model legislation for the Australian Capital Territory to regulate the use of listening devices, should encourage uniformity of approach and standards between the States in the use of such devices, and

d. these recommendations should be effected as a matter of urgency.

A Telecommunications Interception Agency

6.20 The Committee has already concluded, in its consideration at Chapter 3, that:

a. that there is a requirement for information from telecommunications interception to be extended so that the State and Northern Territory Police forces, the NCA and the NSW Drug Crime Commission have rapid access to information on serious drug crimes;

b. that the case to extend to the NCA, State and Northern Territory Police forces and the NSW Drug Crime Commission the power to intercept telecommunications has not been made;

c. that essential rights to privacy and to protection from illegal interception and the malicious use of intercepted material are best preserved by restricting to the minimum the number of agencies legally empowered to effect interception;

d. that a Telecommunications Interception Agency should be established to carry out all interceptions for the AFP, the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission;

e. that all intercepts should continue to be made through Telecom;

f. that the Telecommunications Interception Agency should be established within the AFP as it is best placed to conduct the interceptions for all authorised agencies, and can guarantee a career structure for officers and maximum staff turnover;

g. that each law enforcement agency should retain the full power to select targets, determine priorities, appraise Telecom, prepare draft warrants and approach Federal Court Judges seeking the issue of the warrants;

h. that while the legal right to target interceptions should be extended and decentralised, once the warrant is issued the interceptions should be carried out by a single agency, on a regional basis if economically justified;

i. that the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission should each be offered lines for telecommunications interception on a full cost-recovery basis and each law enforcement body should have the power to determine the priorities for the use of lines rented, and

j. that this extension of access to intercepted information to the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission must be accompanied by stringent centrally co-ordinated safeguards, recognising at the same time a requirement for administrative efficiency and the need for a fast-track mechanism for urgent interceptions to exist with subsequent justification.

6.21 Although not directly referred to in the Committee's terms of reference, the question of control of interceptions comes within the ambit of the Committee's requirement to report on, among other things, 'the appropriateness of the mechanism for conducting interceptions'. Furthermore, the Attorney-General told the House of Representatives during his second reading speech that this Committee should report 'on the feasibility of having a central Commonwealth agency to carry out interceptions for other authorities'.[15]

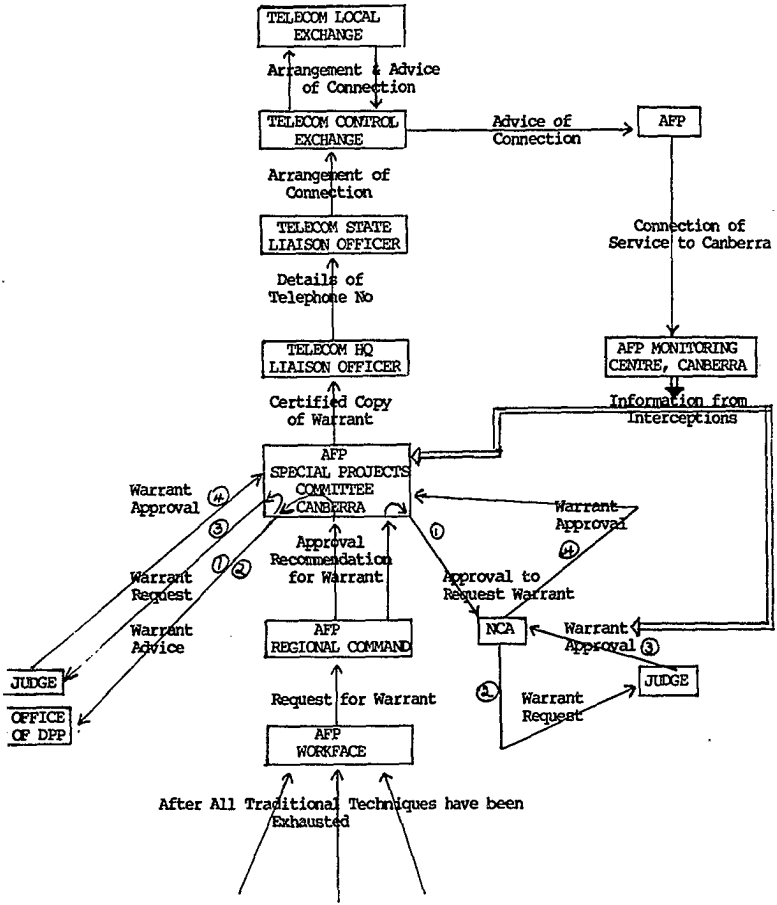
6.22 The present organisational method of conducting interceptions is illustrated at Figure 6.1. Justice Stewart examined this system and reported as follows:

> The Commission is of the view that the current system for the authorisation of the installation of interception devices and the subsequent monitoring of intercepted telephone conversations is cumbersome, slow and urgently in need of review.[16]

6.23 The Committee is satisfied, from the evidence put before it, that the present system creates unacceptable delays. The Committee accepts that the assessment of priorities for interception by an authorised agency should be determined solely by that agency. It follows that, in a system in which the physical implementation of interception is centralised, the interception agency should not act to filter interceptions, in either the application process or the subsequent return flow of targetted information.

FIGURE 6.1

MODEL 1 : PRESENT SYSTEM



6.24 While accepting that a centralised control system is essential, the Committee does not preclude the possibility that a telecommunication interception agency might decentralise its operations into regions of operation, based perhaps in Sydney and Melbourne and other cities as required on an ad hoc basis. The central agency would act in a co-ordination role only, and would have no assessment role as in the present system. An outline organisational chart showing the flow of requests and information under this form of centralised implementation is shown at Figure 6.2. Figure 6.3 illustrates the system proposed by the Bill, in which up to 11 different agencies could be authorised to effect interceptions. The Committee rejects this system, for the reasons outlined.

6.25 The centralised control of interceptions was not well supported by those State police who gave evidence to the Committee, by the Australian Federal Police or by the National Crime Authority, which was particularly critical of the proposal:

> In summary, the Authority is firmly of the view that a centralised agency to conduct and monitor telephone interceptions is inappropriate. For reasons of security and efficiency, the Authority would be loath to entrust physical surveillance or the monitoring of listening devices to another agency. It is difficult to see why telephone interceptions should be treated differently.[17]

6.26 Mr Justice Stewart was opposed, in principle, to any central organisation effecting interceptions for other authorised agencies:

FIGURE 6.2

MODEL 2 : CENTRALISED SYSTEM AFTER AN EXTENSION OF ACCESS

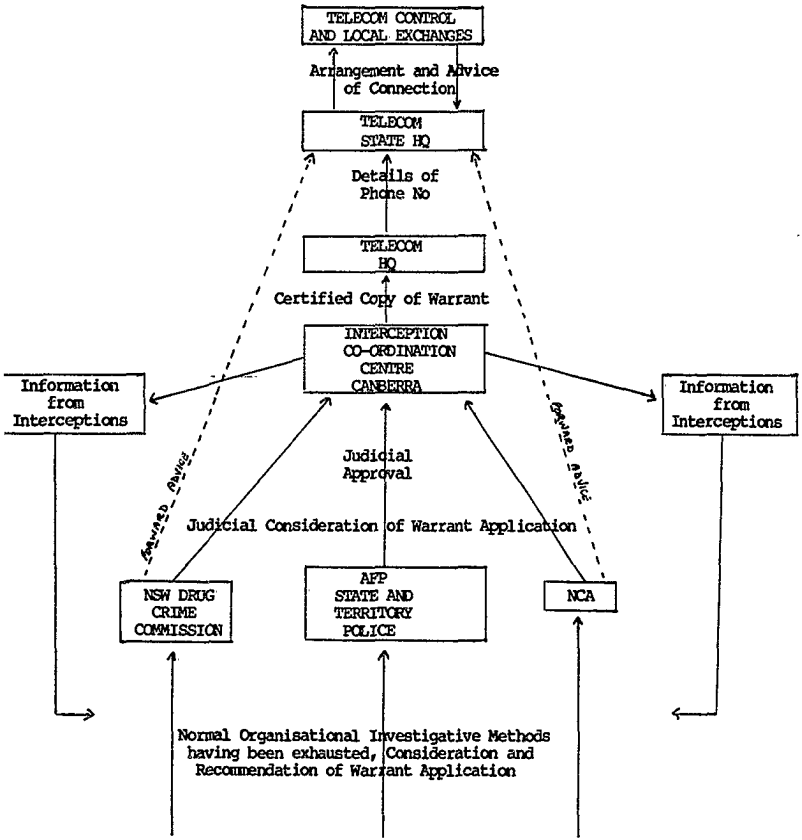
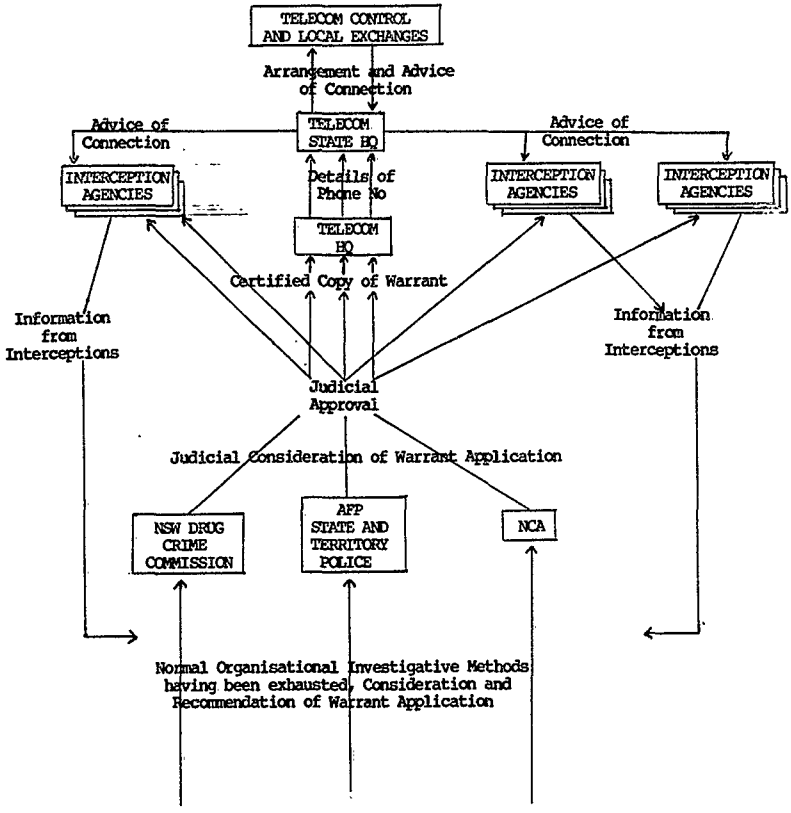


FIGURE 6.3

MODEL 3 : DECENTRALISED SYSTEM AFTER AN EXTENSION OF POWERS



> There is a conflict of interest situation. There is always a difficulty where a body has a function to perform itself and some other body is asking it to take away some of its own resources to do something for another body. That is the problem we are experiencing with the AFP. We are not suggesting that the AFP is being unfair but the AFP has to put itself in a situation of being the judge and jury in relation to competing priorities. The NCA would not want that situation to occur. Those are the main arguments why I would not want to see the NCA set up as a centralised agency. The same arguments apply to any agency, whether it is the NCA or not.[18]

6.27 The NSW Police were also opposed to a centralised agency, largely on grounds similar to Mr Justice Stewart, that there would be a competition of priorities for implementation:

> We would not support, say, a centralised Federal model, mainly because we would then be competing with other States for priorities all the time and it would make planning of operations practically impossible, because we are not au fait with what every other force is doing from day to day, although we have a strong co-operation with them. Secondly, the lines of communication are stretched ... We could run it a lot better if we had the operation here in Sydney.[19]

6.28 But the NSW Police did not oppose a form of decentralisation:

> That means the actual tapes and everything would be in Sydney. Yes, that would overcome that major objection. It is very costly having it in Canberra where the lines have to run backwards and forwards from whereever the tap is on.[20]

6.29 The Victorian Police witness told the Committee that, in principle, he would have no objection if the AFP were to conduct all interceptions or a centralised basis. But there could be security problems:

> ... it is very difficult to run a tight investigation or a task force investigation without there being some sorts of leaks occurring and, if leaks occur, then you are going to put other people in an embarrassing situation where all they did was install a telephone intercept for you somewhere. It is better to keep it within your own organisation if you possibly can. We work on a need to know basis - in other words, anybody who is not concerned with the investigation needs to know nothing about it; that is the situation. Whilst I in principle would have no objection to it, you are putting the AFP into a difficult situation and on top of that they would need to provide resources where the States will benefit.[21]

6.30 Evidence such as this was weighed very carefully by the Committee. Elements of the arguments against centralising interception have considerable validity, but the Committee found it necessary to be wary of the 'tribal' or 'territorial' imperative which appeared close to the surface of many of the points made to the Committee by the various police witnesses. Rivalries and jealousies between State police forces, and between State and Federal police, have a long history in this country. Mr Justice Stewart himself, in his Report on Drug-Trafficking, referred to the fragmented and primitive nature of national police intelligence, and highlighted the lack of co-operation in the history of police relations, saying that 'total police effectiveness will never be obtained in Australia unless co-operation between the Australian Federal Police force and the State forces is significantly improved.'[22]

6.31 It was even suggested to the Committee by one witness, Mr Richard Hall, that a centralised interception unit, jointly staffed by Federal and State police, may in fact act to foster police co-operation:

> I think we need the tightest possible control of phone tapping. You can do it, as I would suggest, quite consistently, in acting against organised, serious, major crime in the State.

> There is one bonus, by the way, about this kind of Federal unit and a strong joint State role, with State people being in there, and that is that I am firmly convinced that anything that goes towards encouraging a real and closer co-operation between the police forces of Australia is absolutely useful. The problem about them is that there have been often competing baronies; it has been riddled by the most boring things such as State jealousies. It has also been riddled by suspicion and mistrust, some of it stemming from corruption real and suspected in rival forces. Really, one of the divisions you can get ... and this is really a very debilitating factor in the contesting of crime in Australia, is this State jealousy. If you can get a really genuine Federal-State co-operation, strongly controlled in one place in Canberra, I think it would be a real contribution.[23]

6.32 Centralisation of interception was strongly supported in the submission of the Victorian Bar which highlighted the difficulties inherent in a system which permitted a multiplicity of agencies operating independently. It further argued that a centralised system would facilitate the enforcement of all necessary safeguards:

> Thus the task of ensuring that the Act was being complied with and that appropriate safeguards were in place would be greatly simplified. Each agency conducting telephone intercepts would be supervised through their nominated representative who would be a member of the central body. Such a legislative scheme would in our submission go some distance towards achieving both the objects of providing meaningful safeguards and at the same time developing an efficient mechanism for obtaining and conducting intercepts free of existing bureaucratic constraints. There ought to be a central register of issued warrants with reporting requirements of progress in a way that would render continuing surveillance subject to an ultimate accountability. Only thus can one have some assurance that the system is not being abused.[24]

6.33 The Committee endorses this view. The Committee believes that the privacy invasive nature of telecommunications interception and the need to ensure that interception powers are not abused demand the tightest possible control, and that this can not be achieved with a possible 11 different agencies capable of effecting interceptions. The Committee recognises the validity of the argument that a central agency may be forced to assess competing priorities, as in the current system. However, the Committee believes that a system can be devised which facilitates rapid access to intercepted information by authorised agencies, ensures the application of necessary safeguards and permits authorised agencies to determine their own priorities which would simply be implemented, not assessed, by the interception agency. Such a system would ensure that authorised agencies would receive only the information for which authority had been granted in the particularity of a warrant.

6.34 Early in the inquiry, the Committee conducted an inspection of the AFP's Special Projects Branch, and observed the nature of its operations. As noted in Chapter 1, the Committee was impressed by the procedures presently implemented by the AFP. Under a new system which removed the assessment role for the Special Projects Committee in non-AFP-requested interceptions, the Committee believes that much of what Justice Stewart found were cumbersome procedures and delay factors would be removed.

6.35 Accordingly, the Committee concludes that:

a. a telecommunications interception agency should be established within the AFP for the implementation of all interceptions, though the Australian Telecommunication Commission, on behalf of authorised agencies such as the National Crime Authority, State and Northern Territory Police Forces, the NSW Drug Crimes Commission and the AFP itself;

b. that the agency should effect approved warrants immediately on receipt, using leased lines permanently allocated to

respective agencies, each agency determining its own priorities for the lines allocated;

c. that the agency should be directed to forward by the fastest secure means to requesting authorised agencies only that information expressly authorised by warrant;

d. that authorised agencies should be invited to second staff to the interception agency;

e. that staff allocated to the interception agency should be rotated regularly, to protect the integrity of the agency;

f. that all interceptions should be conducted on a full cost-recovery basis charged to requesting agencies, and

g. that the interception agency should conduct its operations on a regional basis, depending on cost, demand and experience.

Safeguards and Protections

6.36 The Committee has, throughout this report, accepted the argument that access to information from telecommunications interception is a necessary weapon in the arsenals of law enforcement agencies and those charged with the assessment of internal threats to national security. The Committee has been at pains to stress, however, its qualifying view that interception by law enforcement agencies can be justified only under very tightly defined circumstances, and should be effected only through a single agency operating to stringently defined safeguards. The Committee has already concluded that an interception agency based on the Australian Federal Police model would be appropriate to conduct all interceptions for law enforcement agencies, on priorities determined solely by those agencies, on a full cost-recovery basis.

6.37 The distinction between the requirements of law enforcement agencies and security intelligence agencies for intercepted information, and the consequent differences in the use to which this information is put, is a fundamental one. Furthermore, the potential for privacy invasion by a multiplicity of law enforcement agencies is much greater than by a single security agency effecting interception under close Ministerial scrutiny for tightly defined purposes related to national security. The Committee is satisfied that the present arrangements under which the Australian Security Intelligence Organisation conducts its interceptions are satisfactory. The remaining part of this Chapter discusses the Committee's views on necessary safeguards for the conduct of interceptions and the access to, and use of, resultant information by law enforcement agencies alone.

6.38 Earlier in this Chapter the Committee indicated that re-drafted legislation is necessary, incorporating both the revised provisions as recommended in this report and the original framework provisions of the principal Act. Reference has already been made to some safeguards and protections considered necessary by the Committee. In this part of the Chapter, key safeguards and protections the Committee considers essential in a revised law enforcement interception framework are brought together. These are discussed under the following broad headings:

a. justification - including the warrant procedure and the limitations on the use of interception;

b. implementation - including the mechanism through which interception should be effected;

c. communication and use of intercepted information - including the admissibility of evidence and flow of non-warranted information between agencies;

d. post-interception reporting - including requirements for reporting-back arrangements to warranting judges, and ministerial reports to Parliament, and

e. independent audit and scrutiny - for both law enforcement agencies and the Australian Security Intelligence Organisation.

Justification

6.39 The Committee finds that telecommunications interception is justified in only very limited and closely defined circumstances. As argued in Chapter 4, these are:

a. murder;

b. kidnapping, and

c. organised crime associated with offences:

(1) that involve 2 or more offenders and substantial planning and organisation, and

(2) that involve, or are of a kind that ordinarily involve, the use of sophisticated methods and techniques, and

(3) that are committed, or are of a kind that are ordinarily committed, in conjunction with other offences of a like kind, and

(4) that involve kidnapping, murder or serious drug trafficking offences and associated financial dealings in each case,

or which relate to conspiracy to commit any of the above offences.

These offences are referred to in subsequent paragraphs as "relevant offences".

6.40 The authority to issue warrants to intercept should be restricted to Judges of the Federal Court of Australia. In considering an application for a warrant, a Judge should be satisfied that:

a. there are reasonable grounds for suspecting that the nominated telephone service is being, or is likely to be, used by a person who is suspected, on reasonable grounds, of

(1) committing;

(2) having committed;

(3) being about to commit, or

(4) conspiring to commit

a relevant offence;

b. other investigative techniques have either been exhausted or would, in the circumstances, be inappropriate, and

c. information likely to be obtained from the warrant would materially assist in the investigation of a relevant offence that the person is suspected, on reasonable grounds, of

(1) committing;

(2) having committed;

(3) being about to commit, or

(4) conspiring to commit.

6.41 The revised legislation should provide that a warrant application must be in writing, sworn, and specify with particularity the nature of the offence and the person and place to be the subject of interception. A warrant application should also include:

a. the identity of the law enforcement officer applying for a warrant, and the identity of the authorising officer;

b. a statement of the time for which an interception is sought, and a justification for any application extending to the maximum warrant period of 90 days, with a statement establishing why the interception of successive communications is considered necessary, and

c. a statement of previous interceptions sought or effected which involved the same person, telephone service or place, with the results of such interception.

6.42 An authorised agency should be enabled to apply by telephone to a Judge for the issue of a warrant, but only in the most urgent circumstances, provided that within one working day of the issue of a warrant by telephone, the applicant provides the issuing Judge with a sworn affidavit containing the full information necessary for a normal application for a warrant.

Implementation

6.43 Warrants should be valid for a period not exceeding 90 days, and a chief officer of an authorised agency (e.g. State police or the National Crime Authority) should be required by law to discontinue interception and revoke a warrant as soon as the grounds on which a warrant was issued no longer exist. Although under present legislation the AFP may effect interception without recourse to Telecom and may also enter premises, the Committee believes that standard provisions should apply to all agencies. Warrants should not authorise any entry upon premises and must

authorise interceptions only through the Australian Telecommunications Commission (Telecom). Copies of all warrants and instruments of revocation should be forwarded to the Managing Director of Telecom and retained in the records of each respective authorised agency.

6.44 Legislation should provide that, in the implementation of interceptions, legal professional privilege is protected. The Canadian Privacy Act as amended to 1977 provides the following model:

> (1.1) No authorization may be given to intercept a private communication at the office or residence of a solicitor, or at any other place ordinarily used by a solicitor and by other solicitors for the purpose of consultation with clients, unless the judge to whom the application is made is satisfied that there are reasonable grounds to believe that the solicitor, any other solicitor practising with him, any person employed by him or any such solicitor or a member of the solicitor's household has been or is about to become a party to an offence.
>
> (1.2) Where an authorization is given in relation to the interception of private communications at a place described in subsection (1.1), the judge by whom the authorization is given shall include therein such terms and conditions as he considers advisable to protect privileged communications between solicitors and clients. [25]

6.45 As outlined earlier in this Chapter, legislation should provide for a telecommunications interception agency to effect all interceptions and monitor/transcribe intercepted communications on behalf of all authorised agencies. The proposed eligible agencies are the AFP, State and Territory Police forces, the National Crime Authority and the NSW Drug Crime Commission. At the request of a State Premier or the Chief Minister of a Territory, the Attorney-General of the Commonwealth should prescribe by way of regulation to the Act that an eligible

authority be declared by the Attorney-General an authorised agency to initiate warrants for interception. Legislation should require the Attorney, before making such a proposal, to be satisfied that State/Territory legislation has made adequate provision:

a. for the retention of warrants and instruments of revocation by the authorised agency of the State or Territory;

b. requiring the authorised agency to keep and retain proper records relating to interceptions, the use made of intercepted information and the communication and destruction of intercepted information;

c. requiring the authorised agency to keep records of intercepted communications in a secure place;

d. for the regular inspection of records by an independent authority and for the reporting by that authority to the relevant State or Territory Minister of the results of each inspection and the extent of compliance with the requirements of the State law and with the provisions of federal law;

e. for the relevant State or Territory Minister to furnish to the Attorney-General copies of all reports by the independent authority;

f. for the chief officer of the eligible authority to furnish to the State or Territory Minister copies of all warrants and instruments of revocation and, within 3 months after the expiration or revocation of a warrant to report to the State or Territory Minister on the use made of intercepted information and the communication of that information;

g. for the State or Territory Minister to furnish to the Attorney-General copies of all warrants and instruments of revocation and a report in writing

describing in general terms the use and communication of information obtained by virtue of those warrants, and

h. for the destruction of irrelevant records and copies of intercepted communications.

6.46 Before making a proposal to the Parliament, the Attorney-General should also be satisfied that the State or Northern Territory has entered into an agreement to pay all expenses connected with the issuing of warrants and the interception of communications by the telecommunications interception agency and to reimburse all expenses incurred in connection with those warrants.

6.47 Federal legislation should also empower the Attorney-General to revoke a declaration where the relevant State or Territory law is not maintained; where compliance with the law is unsatisfactory; where the agreement in relation to the payment of expenses ceases to operate or is unsatisfactorily observed; or where there is not satisfactory compliance with the provisions of federal law. A declaration should also be able to be revoked at the request of the relevant Premier or Chief Minister.

6.48 Provisions for the Australian Federal Police and the National Crime Authority should be identical, and be no less stringent than those applicable to other authorised agencies. Ministerial reporting responsibility should rest with the Special Minister of State.

Communication and Use of Intercepted Information

6.49 The Committee concludes by majority that re-drafted legislation should provide that information obtained in contravention of legislation covering interception should be inadmissible as evidence in court, except solely for the purpose of establishing a contravention. As contained in the subject

Bill, there should also be open to defendants a remedy to object to evidence from intercepted information by establishing a breach of the re-drafted legislation "on the balance of probabilities".

6.50 Further, the Committee believes that the legislation should provide for pre-trial hearings to ascertain the status of evidence, along the lines of the following extract from relevant US legislation (18 USC 2518 (10) (a)):

> (10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that -
>
> (i) the communication was unlawfully intercepted;
>
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
>
> (iii) the interception was not made in conformity with the order of authorization or approval.
>
> Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.[26]

6.51 Under the interception arrangements proposed earlier in this Chapter, the telecommunications interception agency would be able to communicate to an authorised agency the results of that agency's requested interception, that is, only that information particularised in the warrant obtained by the authorised agency. The communication of any legally intercepted information other than that requested by warrant should be prohibited, unless it relates to an offence punishable by imprisonment for 3 years or longer. There should be no exceptions to this provision.

6.52 The Committee further concludes that penalties for misuse of legally obtained information from interceptions should be at least as stringent as those applicable to offences related to illegal interception, except for technical breaches.

Post-interception Reporting

6.53 Re-drafted interception legislation should strengthen the safeguards inherent in a system of annual Ministerial reports to the Parliament, following periodic reports which would include reports:

a. from authorised agencies to the interception agency;

b. from the telecommunications interception agency to the Special Minister of State, and

c. from State/Territory Ministers to the Special Minister of State describing in general terms the use and communication of information obtained from interception warrants.

6.54 The Special Minister of State should be required by law to report annually to the Parliament. Subject to the non-disclosure of information prejudicial to current investigations, the Minister's annual report should include:

a. the number of applications made for the issue of warrants, by authorised agency and in total;

b. the number of applications made for extension of warrants, by authorised agency and in total;

c. the number of applications referred to in sub-paragraphs a and b that were granted, the number of such applications that were refused, and the number of applications that were granted subject to terms and conditions;

d. the average period for which warrants were given and for which renewals and extensions were granted;

e. the number of warrants that, by virtue of one or more renewals thereof, were valid for more than 90 days, for more than 150 days, and for more than 180 days;

f. the offences in respect of which applications for warrants or extensions of warrants, were granted, specifying the number of warrants given in respect of each offence;

g. a general description of the interceptions made under such warrants or renewals, including:

   (1) the approximate nature and frequency of incriminating communications intercepted;

   (2) the frequency of other communications intercepted;

   (3) the approximate number of persons whose communications were intercepted.

h. in relation to the interceptions made under warrant and renewals, the approximate nature, amount and cost of the manpower and other resources used in the interceptions;

i. the number of persons identified in a warrant

(1) who were arrested, or

(2) against whom proceedings were commenced in respect of:

(a) an offence specified in the warrant,

(b) an offence other than an offence specified in the warrant but in respect of which an authorisation may be given; and

(c) an offence in respect of which a warrant may not be given;

j. the number of persons identified in a warrant

(1) who were arrested, or

(2) against whom proceedings were commenced in respect of:

(a) an offence specified in such a warrant;

(b) an offence other than an offence specified in such a warrant but in respect of which a warrant may be given, and

(c) an offence other than an offence specified in such an authorisation and for which no such authorisation may be given

and whose commission or alleged commission of the offence became known as a result of an interception of a private communication under a warrant.

k. a statement showing the maximum, minimum and average periods of time between the issue of warrants and the implementation of interceptions.[27]

6.55 The Committee received evidence which argued that the reporting provisions in the legislation should include a requirement to "report-back" to the Judge who issued a warrant on the progress of an authorised interception. It was argued that such a requirement could be levied at such intervals as an issuing Judge may determine, and should include a justification for continued interception. On the expiry of a warrant, a final report should be made to indicate the results obtained from the interception.

6.56 The Committee considered this argument at length, and weighed its merits. A balanced judgment was necessary, as in many other areas of the Committee's inquiry. On one hand, such a procedure would facilitate a more thorough comprehension by warrant-issuing authorities of the nature, extent and likely results of interception. On the other hand, such a requirement would create a further non-judicial function for judicial officers. It might also detract from the primary relevant responsibilities inherent in Australian democracy, that of an agency head to a Minister, and that of a Minister to the Parliament, under the reporting provisions outlined earlier in this part. On balance, the Committee rejected the suggestion of a reporting-back mechanism.

Independent Audit and Scrutiny

6.57 The last major grouping of safeguards considered necessary in a revision of interception law centres on a need for independent audit and scrutiny. Under the proposed legislation, a requirement was included for State authorities permitted to intercept telecommunications to be subject to provisions:

> for the regular inspection of records by an independent authority and for the reporting by that authority to the relevant State or Territory Minister of the results of each inspection and the extent of compliance with

> the requirements of the State law and with the provisions of the Telecommunications (Interception) Act.[28]

6.58 The Committee concludes that safeguards no less stringent than these should be incorporated in new legislation to extend access to intercepted material. The Committee believes that independent audit and scrutiny should apply to all law enforcement agencies involved in interception, and that the interception operations of the Australian Security Intelligence Organisation should also be periodically audited.

6.59 The question of independent audit and scrutiny by an inspector-general was canvassed with key agencies during the inquiry. Mr Justice Stewart initially in evidence could not 'in principle, see any objection to it ... to an inspector coming to see what you are doing and making an audit.'[29] On further reflection, however, he advised the Committee that he now did not support the proposition, considering that 'the fact that the warrant would be issued by a judge is a sufficient safeguard at that stage of the interception process and that the reporting requirements proposed ... in relation to the Authority ... are a sufficient safeguard for the remaining stages of the process.'[30]

6.60 The Committee looked at the audit and scrutiny function with regard to ASIO's interceptions when examining Mr A.K. Wrigley, the Director-General of Security. Mr Wrigley was asked whether it would be appropriate for the proposed Inspector-General of Intelligence and Security to audit ASIO's interceptions. He replied:

> Yes, I would think so. One of his functions is proposed to be to establish propriety and legality and to that extent I suppose he might reasonably feel - I would not have any difficulty with the argument - that an audit of telephone intercepts from time to time was a reasonable implementation of that function. I certainly would not have any trouble with his doing it.[31]

6.61 The Assistant Commissioner (Investigations) in the Australian Federal Police, Mr B.C. Bates, was asked a similar question when giving evidence to the Committee. He qualified his response by indicating that he was unprepared to provide AFP policy, but gave a personal view:

> I have no problems whatsoever with that sort of proposition and I would be most surprised if the Commissioner did. I have been in countries where that type of situation exists in terms of facets of law enforcement. I see nothing wrong with it at all.[32]

6.62 Mr Bates elaborated his position:

> In the United Kingdom they work on a wider aspect rather than just telephone intercept, of course, in their internal affairs investigations being conducted by the various county police forces and the metropolitan forces. They have the ombudsman-type person who comes in and does an audit of what is going on. Even in an examination of intelligence they have that sort of situation. My view is that police forces in this day and age have to be accountable. They have to be accountable in every way and so from my point of view I just see no problems whatsoever for that sort of situation.[33]

6.63 The Victoria Police Assistant Commissioner (Crime), Mr P. Delianis, told the Committee that he 'would have no objection'[34] to a proposition that there should be an independent audit. In their evidence to the Committee, however, the New South Wales Police evinced 'a little concern' at proposals for regular inspections by an independent authority. They argued that existing checks and balances, short of independent audit, were quite satisfactory, but that they were 'not adverse to any sensible control mechanism.'[35]

6.64 The Committee was therefore confronted with another "on balance" decision. Because of its concern to ensure the maximum application of safeguards consistent with an efficient system, the Committee inclined to the view that there should be independent audit and scrutiny of the implementation of interception procedures in their totality.

6.65 The Committee concludes that an independent judicial auditor should fulfil this function with respect to law enforcement agencies, assuming that the proposed Inspector-General of Intelligence and Security would independently audit ASIO's interceptions.

Financial Considerations

6.66 The Committee received a limited amount of incidental evidence in relation to the financial implications of extending the powers of telecommunications interception. This evidence is set out in this section.

6.67 Telecom told the Committee that:

> The present cost to the AFP of the permanent leased lines to Canberra from the capital cities is $197,000 pa.
>
> The additional leased line costs to the AFP depends, in the case of each intercept, on the distance between the control exchange and the local exchange and the length of time the intercept is conducted for, ie the temporary leased line costs are based on distance and the length of time the lines are required for. These additional leased line costs can vary in metropolitan areas from under $100 to hundreds of dollars while in country areas can cost thousands of dollars.[36]

6.68 At the beginning of the inquiry, Telecom advised the Committee that a number of factors would have to be taken into consideration in estimating the costs involved if interception powers were extended to State Police. These factors included:

i. whether the interceptions (ie monitoring and recording) took place at a central location for all States (say Canberra) which would involve permanent leased lines from all capital cities. The number of lines involved would depend on perceived State Police requirements;

ii. whether the interceptions were at State locations. The costs involved in these cases would depend on the number of permanent lines required from the State control exchange to the State monitoring centre.

In the case of either (i) or (ii) additional costs would be incurred for the leased lines between the control and local exchanges.[37]

6.69 Telecom made their position clear in stating that 'if interception powers were extended to State Police, Telecom would be reviewing the present charging arrangements in order to reflect the additional administrative and labour costs involved'.[38]

6.70 The AFP, in evidence to the Committee, detailed the resource and cost factors involved in current AFP interception operations:

> The AFP currently has the capacity in terms of available equipment to monitor 38 telephones. However, staffing and financial constraints and experience have effectively limited monitoring to an average of 15 intercepts at any one time.
>
> To effectively manage and maintain 15 intercepts on a continuous 24 hour a day basis, there is a staffing requirement currently committed by the AFP of:
>
> 1 Superintendent
> 1 Chief Inspector
> 4 Station Sergeants
> 1 Sergeant
> 24 Constables

Any increase in the number of interceptions carried out by the AFP would of course require staffing adjustment on the basis that one member can handle between 3 and 5 intercepts per shift (there are 3 shifts in a 24 hour period).

The cost of leasing land lines from Telecom varies from State to State but the average is $7,000 per line. It is necessary for a number of lines in the majority of States to be instantly available so that no delays occur once a warrant is issued. This necessitates leasing expense *regardless of operational demand*. Presently the cost of maintaining sufficient leased lines is over $230,000 per annum.

To forecast the cost of an interception is difficult. Taking into account, however, monitoring equipment, computers, word processing equipment, support staff, consumables, power, Telecom line hire, but excluding capital costs, the annual cost per intercept is approximnately $75,000.[39]

6.71 At the Committee's request, Telecom provided a preliminary assessment of likely costs involved in establishing additional interception facilities:

i. installation charges for the interface equipment - approximately $2,150;

ii. annual costs for permanent leased lines from the control exchange to the monitoring centre - installation charges $3,000 and $6,000 annual rental (based on a requirement for 20 lines and the assumption that the monitoring centre would be in the capital city concerned).

The AFP has provided the interface equipment for the various control exchanges and information on the cost of providing the equipment for other organisations would need to be obtained from the AFP. It is understood, however, that AFP development costs were in the order of $15,000 and the cost of manufacture of additional equipment (15-30 lines) is approximately $400. The cost to other organisations would depend on:

i. whether there is spare capacity in the present interface equipment which could be utilised by other organisations;

ii. the basis on which the AFP would supply new equipment, for example, it may wish to recover some of its development costs.

Ongoing costs (based on present charges) would be the leased line costs which depend, in the case of each intercept, on the distance between the control exchange and the local exchange and the length of time the intercept is copnducted for, ie the temporary leased line costs are based on distance and the length of time the lines are required. These additional leased line costs can vary in metropolitan areas from under $100 to hundreds of dollars while in country areas can cost thousands of dollars.

The following are examples of temporary leased line costs incurred by the AFP over the last 12 months:

PERIOD OF INTERCEPT	DISTANCE INVOLVED KM	COST $
7 days	7.5	137
16 days	5	75
1 month 17 days	44	930
2 months	12.5	409
3 months	6	480
3 months	22.5	1,083
3 months	94	2,000
3 months	1390	6,250
6 months	5	852

Telecom is at present looking at introducing standard fees for providing the temporary facilities for intercepts. On possibility is to charge standard fees on a weekly basis in the following categories:

- Metropolitan areas
- Outer metropolitan areas
- Country areas

This would simplify the charging arrangements and enable the various organisations involved to know at the outset what the charges will be for each intercept. However, it will be some time yet before Telecom completes its studies.[40]

6.72 The Committee draws no conclusions from this incidental evidence received during the course of the inquiry. The evidence is set out as received to enable a consideration to be made of the Committee's substantive conclusions and recommendations with some of the financial implications in view.

(S.P. Martin, MP)
Chairman
20 November 1986

ENDNOTES

1. Evidence, p 903

2. Exhibit 26, p 2.

3. Evidence, p 1089.

4. Submission No 39, The Victorian Bar, pp 6-7.

5. Evidence, pp 881-882.

6. Evidence, p 886.

7. Evidence, p 870.

8. Australian Law Reform Commission, (ALRC) Report No 22, Privacy, p 366.

9. Evidence, p 888.

10. Judgement No 3507 of 1986, Mr Justice Dowsett, Supreme Court of Queensland: Robin Howard Reichelt, plaintiff, v. Sir Terrence Murray Lewis, Commissioner of Police, defendant, p 24.

11. Submission No 41, Queensland Law Society, p 3.

12. Submission No 41, Queensland Law Society, p 5.

13. Submission No 42, Law Council of Australia, p 18.

14. ALRC, Privacy. p 366.

15. H R Deb (4.6.85) 4596.

16. Stewart, Report, p 303.

17. Evidence, p 453.

18. Evidence, p 470.

19. Evidence, pp 528-529.

20. Evidence, p535.

21. Evidence, p 422.

22. Stewart, Report - Drug Trafficking, p 516.

23. Evidence, pp 844-845.

24. Submission No 39, The Victorian Bar, p 5.

25. Cited in Submission No 1, Senator N Bolkus, pp17-18.

26. Cited in Submission No 1, Senator N Bolkus, pp24.

27. Adapted from Submission No 1, Senator N Bolkus, pp12-13.

28. Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 1986, p29.

29. Evidence, pp499-500.

30. Submission No 38, National Crime Authority, p3.

31. Evidence, p340.

32. Evidence, p106.

33. Evidence, p107.

34. Evidence, p423.

35. Evidence, p540.

36. Evidence, p237.

37. Evidence, p238.

38. Evidence, p238.

39. Evidence, pp85-86.

40. Submission No 34, Telecom Australia, pp5-6.

DISSENTING REPORT OF SENATOR BRIAN ARCHER, MR PHILIP RUDDOCK, MP, AND MR PETER MCGAURAN, MP

Overview

> This Commission has not the slightest doubt that organised criminal activity is continuing which has not yet been identified by conventional law enforcement methods.[1]

1. So found the Hon Mr Justice Stewart while conducting the Royal Commission of Inquiry into Drug Trafficking. It is our firm belief that for this situation to be reversed, law enforcement agencies must be given every possible means to counteract serious crime.

2. On 2 April 1985 the Special Premiers' Conference on Drugs, held in Canberra, endorsed:

> the importance of achieving full co-operation between law enforcement authorities both within jurisdictions and between jurisdictions. The Conference called on all relevant authorities to ensure that they work together in a co-operative way.

3. Further the Conference agreed that:

> telephone interception powers can be a valuable aid in investigation of drug trafficking. The Commonwealth will extend such powers in relation to drug trafficking to the States, subject to stringent controls being exercised over their use. The controls will include a requirement for judicial warrants.

4. The Committee's report acknowledges the arguments for and against each of its conclusions and reaches on balance, judgements to extend both the range of circumstances in which telecommunications interceptions may occur and access to information so gained to a wider class of law enforcement agencies.

5. As part of its package of proposals, the Committee, by a majority:

a. limits quite seriously the possible range of offences in which telephone interceptions may be used to investigate breaches in the law;

b. confines use of telecommunications interceptions directly to the Australian Federal Police (AFP) or a Telecommunications Interception Agency of the Commonwealth; and

c. implements the range of additional reporting and safeguard provisions.

6. We believe that a greater weight should have been placed on the arguments advanced by law enforcement agencies for assistance in obtaining evidence which would aid them in obtaining convictions for 'serious drug trafficking offences' and organised criminal activity. In addition, it would assist the National Crime Authority (NCA) in particular to gather general criminal intelligence.

7. It is our view that the extension of telecommunications interception powers should be extended to the NCA, State Police forces and the Northern Territory Police force, desirous of it and the New South Wales Drug Crime Commission. The extension would proceed if requested by the agencies and in accordance with the guidelines first proposed by the Goverment in its amending Bill. (See Chapter 2)

8. We are not in favour of the introduction of a further intervening statutory authority as proposed in the report. As a consequence of this view, we believe that if the law enforcement agencies cited above so request a capacity to utilise telecommunications interceptions, the approach to obtaining a judicial warrant should be accessible and convenient. Warrants should be obtained through State Supreme Court Judges in addition to Judges of the Federal Court of Australia. The interceptions would be facilitated by Telecom.

9. Whilst we broadly accept the majority view as to the range of serious offences for which telecommunications interceptions might be used, like the majority, we recognise that circumstances may arise which we have not envisaged where it may be appropriate that the interceptions power be extended beyond the specified list of serious offences. We believe that it should be possible to obtain an extension to this list expeditiously. We are concerned that if an amendment is required to an Act of Parliament, the system proposed would be a significant impediment to the use of telecommunications interceptions in appropriate cases. We have, therefore, come to the view that whilst the extension of the list should be scrutinised by Parliament, a more appropriate mechanism is the regulation making power.

10. In the area of safeguards like the majority, we accept that the use of telecommunications interceptions does carry significant risks, particularly to privacy. Therefore the use of this power should be balanced with carefully structured safeguards. However the safeguards should not be so stringent as to seriously impede the appropriate use of the power to make telecommunications interceptions.

11. We are of the view that the use of information obtained from interceptions, carried out in accordance with the law, ought to be used in all but the most minor offences. It is our view that the Committee's recommendations to limit the use of such information to a range of offences punishable only by imprisonment for three years or longer, provides a formal and technical defence to charges which ought to quite properly lead to a conviction on available interception evidence.

12. Coupled with this, we find that the majority view which is that information obtained because of some technical contravention of the interception legislation should be inadmissable in a court except solely for the purposes of

establishing a contravention, is in itself an unreasonable requirement. It merely establishes another form of technical defence to offences that could otherwise be properly established and lead to a conviction.

13. The Committee's report envisages a rewriting of the legislation and that the Bill and Act be withdrawn and redrafted. From experience we conclude that this will be a very time consuming procedure. The adoption of this approach might well delay by possibly a year or more the introduction of appropriate legislation. It is our view that the Government should amend the Bill immediately in accordance with the recommendations of the Committee, taking into account the views of this dissent and proceed to put in place the new arrangements as quickly as possible. The Government could then proceed to introduce an amending Bill consolidating both the amendments and the existing legislation at a later date. In order to satisfy the desire of those who would like such legislation in the Parliament quickly, a sunset clause in the amending Bill could be utilised.

14. Finally, it is our judgement that the requirement for both detailed and comprehensive reports to Parliament as well as the intervention of a Judicial Auditor is unnecessary and an excessive intervention that may well hinder the effectiveness and use of interceptions. It is our view that only one of the proposals in the Committee report ought to be accepted by the Government. We believe that a Judicial Auditor as proposed would limit the public release of information which may have the unintended consequence of alerting criminals, to some extent, of the methods of operation of law enforcement agencies. The Parliamentary report mechanism is therefore our preferred option.

The Matters At Issue

15. This dissent is therefore directed to the following paragraphs of the report. Paragraphs 2.165, 3.46, 4.39, 6.19, 6.49-6.52, 6.53-6.56, and 6.57-6.65.

Paragraph 2.165 Issue of Warrants

16. In paragraph 2.165 of Chapter 2 the Committee concludes that:

> on the weight of evidence, and to provide as much protection to individual privacy, the power to issue warrants should be restricted to Judges of the Federal Court of Australia.

It is our view that judicial warrants should be available through State Supreme Court Judges in addition to Judges of the Federal Court of Australia. The approach to a Judge to obtain a judicial warrant should be accessible and convenient.

17. The extension of telecommunications interception powers to a wider range of law enforcement agencies will place a heavier workload on Federal Court Judges, and the issuance of warrants is more likely to be required in the State capital cities rather than Canberra.

18. We do not accept the assertion that State Supreme Court Judges are likely to be compromised in hearings if warrants have been issued by a fellow State Supreme Court Judge. Nor do we accept the assertion that 'Judge shopping' will be a likely result. Witnesses tested on this matter were unable to substantiate by evidence that Federal Court Judges were in any way more superior or competent in such matters than Judges of any of the Supreme Courts of Australia.

19. It has been suggested that the limited experience of Federal Court Judges in criminal matters would be an advantage when issuing warrants. This suggestion seems to us to be flawed. If anything the converse, namely considerable experience in conducting criminal trials, would be an advantage in considering the evidence offered in support of a warrant.

Telecommunications Interception Agency

20. Paragraph 3.46 is a key conclusion of the report. All Committee members support sub-paragraph 3.46(a) which asserts:

> that there is a requirement for information from telecommunications interception to be extended so that the State and Northern Territory Police forces, the NCA and the NSW Drug Crime Commission have rapid access to information on serious drug crimes.

21. Sub-paragraphs 3.46 (e) and (k) are acceptable, the latter subject to paragraphs 41-42.

22. We dissent from sub-paragraph 3.46(b) and the consequential sub-paragraphs which argue for a Telecommunications Interception Agency. ie 3.46(d)(f)(h)(i) and vary 3.46 (c)(g) and (j). Our alternative recommendations are detailed as follows:

a. that there is a requirement for information from telecommunication interception to be extended so that the State and Northern Territory Police forces, the NCA and the NSW Drug Crime Commission have rapid access to information on serious drug crimes;

b. that the case to extend to the NCA, State and Northern Territory forces and the NSW Drug Crime Commission the power to intercept telecommunications has been made;

c. that essential rights to privacy are best preserved by the arrangements contained in proposed section 43 of the Bill - Declaration of an Eligible Authority of a State as a Declared Authority;

d. that the State and Northern Territory Police forces, the NCA and the NSW Drug Crime Commission should be able to carry out their own interceptions;

e. that all intercepts be made through Telecom;

f. that each law enforcement agency should retain the full power to select targets, determine priorities, appraise Telecom, prepare draft warrants and approach Federal and State Supreme Court Judges seeking the issue of the warrants;

g. that the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission should each be offered lines for telecommunications interception on a full cost-recovery basis and each law enforcement body should have the power to determine the priorities for the use of lines rented;

h. that the extension of power to the NCA, the State and Northern Territory Police forces and the NSW Drug Crime Commission must be accompanied by stringent safeguards, recognising at the same time a requirement for administrative efficiency and the need for a fast-track mechanism for urgent interceptions to exist with subsequent justification; and

i. that an independent Judicial Auditor should provide audit and scrutiny of the process of interception and implementation of safeguards.

23. There was evidence before the Committee that the NCA already experienced delays in having interceptions handled by the AFP. The intervention of any third party will always introduce some delay which would not occur if relevant law enforcement agencies are empowered to arrange their interceptions.

24. We cannot agree with the Committee's report in regard to the centralised operation, setting up regional offices, nor the inclusion of seconded State Officers into the system. Such practices would leave the system considerably more open to misadventure than a neat tight operation strictly between Telecom and the user authority. Further, the States can make direct arrangements with local Telecom representatives far more expeditiously than through a third party.

25. For the system to work with the greatest security and speed, the less people and the shortest distance is essential. We do not believe that the granting of powers to the NCA, State Police forces, the Northern Territory Police force and the New South Wales Drug Crime Commission would cause a proliferation of interceptions because each of these agencies are predominantly concerned with their restricted boundaries or specialist enquiries.

26. In relation to the question of resources, the matter was not fully investigated as to whether the AFP could or would be involved in any enlarged scheme. The Federal Government has found it impossible to provide adequate resources to keep its existing law enforcement operations efficient. The AFP and the ABCI in particular, suffer gross deficiencies in both manpower and funding. Additional duties for other forces would create considerable difficulties and it is unlikely that special provisions could be made available and/or a service for which the operating unit would have a very low priority. Further we are concerned that no evidence has been put forward to substantiate a case that a central agency would be more cost effective.

27. While it has been suggested that it would be appropriate for the Telecommunications Interception Agency to also be established on a regional basis, clearly it is more appropriate to leave the matter in the hands of law enforcement agencies. This will enable such bodies to make the most economical and appropriate decisions for locating interception facilities.

Paragraph 4.39 Extension of Power to Serious Offences

28. The Committee concluded, by majority, that:

a. a case has been made for police to have ready access to intercepted information in only the most serious offences, as well as serious trafficking offences;

b. the number of serious offences for which intercepted information should be available should be kept to the absolute minimum;

c. serious offences should be defined in the Act;

d. if the incident and nature of offences gives rise to community concern that interception powers ought to be extended to cover further offences this should be reflected by a further amendment to the Act by Parliament; and

e. until Parliament otherwise provides serious offences defined in the Act should be restricted to only:

(i) murder,

(ii) kidnapping, and

(iii) organised crime associated with offences:

(a) that involve 2 or more offenders and substantial planning and organisation; and

(b) that involve, or are of a kind that ordinarily involve, the use of sophisticated methods and techniques; and

(c) that are committed, or are of a kind that are ordinarily committed, in conjunction with other offences of a like kind; and

(d) that involve kidnapping, murder and serious drug trafficking offences and associated financial dealings in each case,

or which relate to conspiracy to commit any of the above offences.

29. These conclusions are acceptable to us as far as they go. We are of the view that circumstances exist and others may arise where it is appropriate that the interception powers be extended beyond the list specified.

30. The Committee's proposal is for any amendment to be by way of an amending Bill. The procedures for introducing legislation into Parliament are already complex and time consuming. All of the processes involved may take years rather than months. This would be a significant impediment to the use of telecommunications interceptions in cases where it would be clearly advantageous to law enforcement agencies.

31. It is therefore our view, that the list should be placed in a Schedule which is capable of being amended by regulation. Such an approach would not preclude scrutiny by Parliament as all regulations must be laid before each House and be capable of being disallowed by a resolution carried by either House within a prescribed time. In providing for such a flexible approach we are conscious of the extent to which organised crime has grown and changed in recent years. The areas of criminal pursuit and methods of operation have often proved to be more adaptable than the speed with which law enforcement agencies can respond.

32. We do not discount the extremely high value we place on privacy, but we must recall that this legislation is only being introduced because 'organised crime is now firmly entrenched in Australian society'. As we have already pointed out the legislation is part of the agreements endorsed at the Special Premiers' Conference on Drugs. The extension of powers to serious offences was offered to and accepted by the States, and clearly it was intended to be of use in the fight against crime.

6.19 A New Bill

33. The Committee recommends in paragraph 6.19 that:

a. the subject Bill be withdrawn;

b. there be substituted for the subject Bill a Bill for an Act to consolidate and re-structure the principal Act, incorporating the applicable provisions of the subject Bill and the recommendations contained in this report;

c. the Commonwealth, through enacting model legislation for the Australian Capital Territory, to regulate the use of listening devices, should encourage uniformity of approach and standards between the States in the use of such devices, and

d. these recommendations should be effected as a matter of urgency.

34. We do not dissent from sub-paragraph 6.19(c) and (d). The former envisages a model ordinance for the Australian Capital Territory on the use of listening devices in a co-operative arrangement with the States and the Northern Territory which might enable uniform legislation if the Commonwealths proposals are seen as a satisfactory model.

35. Our principal concern with the recommendations contained within paragraph 6.19 is that if a new restructured and rewritten Bill incorporating recommendations of the Committee for safeguards and mechanisms for interceptions is to be introduced, that significant further delay will occur in the extension of telecommunications interception powers to the States and the Northern Territory as well as the NCA. It will also delay the implementation of recommendations extending the range of offences for which this resource may be used.

36. The Government, Opposition and the community generally acknowledge that the apprehension of those involved in drug related offences and organised crime is an urgent necessity. The Drug Summit occurred in April 1985. Delay could mean the introduction of appropriate and agreed remedies will have been postponed by some 2 and 1 half years and possibly longer. We find this delay unconscionable.

37. With the tabling of this report we would like to see the major recommendations upon which there is agreement in place in the Autumn session of 1987. This can only be achieved by

ammending the Bill presently before the Parliament. In order to encourage prompt consideration and drafting of a restructed, redrafted and consolidated Bill for an Act, a sunset clause in the amending Bill could be utilised. Thus the new arrangements could be effected quickly while a more comprehensive approach could be considered properly by the Government's advisors and then introduced in a timely fashion.

Paragraph 6.49-6.52 The Communication and Use of Intercepted Information

38. The report of the Committee recommends restrictions in two circumstances of information obtained by telecommunications interceptions. The circumstances cover information obtained in contravention of legislation covering interceptions, and information obtained which seem to be in excess of information sought and foreshadowed in a warrant offered for an interception. In the former case it is an absolute ban and in the latter restricted to enable communication to relevant authorities only where it relates to an offence punishable by imprisonment for 3 years or longer. It is our view that each of these restrictions only serves to create technical defences to what might otherwise be proven offences.

39. In paragraph 6.49, the Committee concludes by majority 'that redrafted legislation should provide that information obtained in contravention of legislation covering interception should be inadmissible as evidence in court, except solely for the purpose of establishing a contravention.' It is our view that the use of information allowed in such circumstances should still be capable of being used to substantiate a prosecution.

40. In paragraph 6.51, the restriction limits available information only to that foreshadowed in a warrant in advance of the interception. This is to prevent the use of information obtained by chance even though it is significant evidence in

itself. The view of the Committee was that such information should only be available in cases where a sizeable penalty might be imposed and that there should be no exceptions. It would be particularly pertinent in police disciplinary proceedings where prison sentences would not be involved. It is our view that this is an unreasonable prohibition, and would merely provide a technical defence to charges that would otherwise be sustainable In our view the use of such information to serious charges should be a matter for the good judgement of the relevant authorities.

Post-interception Reporting and Independent Audit and Scrutiny

41. In paragraphs 6.53-6.56 and 6.57-6.65, two mechanisims are provided for monitoring the use of telecommunications interceptions. The former paragraphs provide for a comprehensive arrangement for reporting publically to Parliament and the Government. The latter paragraphs provide for independent audit and scrutiny by a Judicial Officer on the implemention of interception procedures in their totality.

42. It is our view that while improved safeguards are appropriate and have been generally approved in Chapter 6 of the report, these two procedures are designed to cover much the same area, one by providing for Parliamentary scrutiny and the other independent and judicial scrutiny. We firmly believe that use of both mechanisims is an unnecessary duplication. Because public reporting may well make available to targets of interception, in an unintended way, information of the extent and methods of operations of law enforcement agencies, we believe the use of an independent auditor will ensure that the successful use of interceptions is less likely to be compromised.

ENDNOTES

1. The Hon. Mr Justice D.G. Stewart, Report, Royal Commission of Inquiry into Drug Trafficking, February 1983, p773.

2. A Prime Ministerial Communique from The Special Premiers' Conference on Drugs, Canberra 2 April 1985, p4.

3. A Prime Ministerial Communique from The Special Premiers' Conference on Drugs, Canberra 2 April 1985, p5.

INQUIRY INTO TELECOMMUNICATIONS INTERCEPTION

INDEX OF SUBMISSIONS

SUBMISSION NO	PERSON/ORGANISATION	DATED
1.	Senator N. Bolkus Parliament House Canberra ACT 2600	Undated
2.	Commissioner R.A. Grey Australian Federal Police GPO Box 401 CANBERRA ACT 2601	20/8/86
NOTE	Part of this Submission is not authorised for publication and remains confidential	
3.	Ms A. Bradford Hon. Secretary Northlakes Branch ALP 15 Nacooma Rd BUFF POINT NSW 2262	20/8/86
4.	Mr T. Rippon Secretary The Victorian Police Association 43 MacKenzie St MELBOURNE VIC 3000	19/8/86
5.	Mr J. Bennett President Australian Civil Liberties Union 283 Lygon Street CARLTON VIC	25/8/86
6.	Mr S.C. Moon Secretary Telecom Australia 199 William Street MELBOURNE VIC 3000	27/8/86
NOTE	Part of this Submission is not authorised for publication and remains confidential	
7.	Mr S. Rothman Honorary Secretary The New South Wales Society of Labor Lawyers' GPO Box 3085 SYDNEY NSW 2001	26/8/86

8.	Mr R. Smith Chairman Concerned Citizens of Griffith PO Box 1770 GRIFFITH NSW 2680	25/8/86
9.	The Hon Mr Justice Zelling, CBE Chairman Law Reform Committee of South Australia Judges' Chambers Supreme Court ADELAIDE SA 5000	26/8/86
10.	Mr D.G. Francis 9 Harvest Drive DARLINGTON WA 6070	26/8/86
11.	Mr M. Martin Chief of Security Ansett Transport Industries Ltd. 501 Swanston St MELBOURNE VIC 3000	25/8/86
12.	Mr S.I. Miller Chief Commissioner of Police GPO Box 2763Y MELBOURNE VIC 3001	25/8/86
13.	Mr D.M. Lenihan Chief Executive Officer National Crime Authority GPO Box 5260 SYDNEY NSW 2001	29/8/86
14.	Mr T.F. Alton Security Manager Australia Australian Airlines PO Box 2806AA MELBOURNE VIC 3001	29/8/86
15.	Mr J.M. Hartnett Secretary Totalizator Agency Board GPO Box 1943R MELBOURNE VIC 3001	28/8/86
16.	Mr J.K. Avery, A.P.M Commissioner of Police (NSW) 14-24 College Street SYDNEY NSW 2000	Undated
17.	Mr. N.N. Mainwaring Chief Executive Officer The Law Society of NSW 170 Phillip St SYDNEY NSW 2000	27/8/86

18.	Mr T. Rippon Secretary Victorian Police Association 43 Mackenzie St MELBOURNE VIC 3000	Undated
19.	Mr B.R. Howe Secretary Legal Division Police Association of NSW PO Box Q283 Queen Victoria Building SYDNEY NSW 2000	4/9/86
20.	Mr R.W. Harding Director Australian Institute of Criminology PO Box 28 WODEN ACT 2606	25/8/86
21.	Mr T. Robertson Secretary Council for Civil Liberties Box 201 PO GLEBE NSW 2037	1/9/86
22.	Mr S.S. Carter Executive Director Queensland Law Society Inc. GPO Box 1785 BRISBANE QLD 4001	29/8/86
23.	Mr I.M. Musumeci Federal Secretary A.T.E.A. PO Box 472 CARLTON SOUTH VIC 3053	3/9/86
24.	Mr. M. Clemens Chairman Supporters of Law and Order PO Box 18 MALVERN VIC 3144	4/9/86
25.	Mr M.H. Byers Chairman Police Board of NSW PO Box R256 Royal Exchange SYDNEY NSW 2000	1/9/86
26.	Mr P.J. Williams President The Western Australian Bar Association (Inc) 8th Floor, Law Chambers Cathedral Square PERTH WA 6000	3/9/86

27.	Mr Graham Miner Legal Affairs Director QANTAS Airways Limited Box 489 GPO SYDNEY NSW 2001	3/9/86
28.	The Hon. C.J. Sumner, M.L.C. Attorney General South Australia Box 464 GPO ADELAIDE SA 5001	3/9/86
29.	Mr D.A. DeBats President South Australian Council for Civil Liberties, Inc. PO Box 410 NORTH ADELAIDE SA 5006	8/9/86
30.	Mr A.D. McGaurr Secretary Department of the Special Minister of State West Block CANBERRA ACT 2600	12/9/86
31.	Mr J.J. Mulheron A/Co-Ordinator-General Premier's Department PO Box 185 BRISBANE NORTH QUAY QLD 4000	18/9/86
32.	Miss T. Cohen Chairman Privacy Committee Box 6 GPO SYDNEY NSW 2001	18/9/86
33.	Mr J.K. Avery Chairman A.B.C.I. Management Committee Box 45 GPO SYDNEY NSW 2001	15/9/86
34.	Mr B.W. Byrnes Acting Secretary Telecom Australia 199 William Street MELBOURNE VIC 3000	23/9/86
NOTE	Part of this Submission is not authorised for publication and remains confidential	
35.	Mr S.C. Moon Secretary Telecom Australia 199 William Street MELBOURNE VIC 3000	24/9/86

36.	Mr Stephen Mason Secretary The Australian Law Reform Commission Box 3708 GPO SYDNEY NSW 2001	30/9/86
37.	Mr T. Game Member of the New South Wales Society of Labor Lawyers Mirvac Chambers SYDNEY NSW 2000	Undated
38.	Mr D.M. Lenihan Chief Executive Officer National Crime Authority GPO Box 5260 SYDNEY NSW 2001	1/10/86
NOTE	Part of this Submission is not authorised for publication and remains confidential	
39.	Mr A.W. McDonald, Q.C. Chairman Law Reform Committee The Victorian Bar 205 William St MELBOURNE VIC 3000	13/10/86
40.	Mr J.D.Maclean Assistant Secretary External Relations Branch Department of Communications PO Box 34 BELCONNEN ACT 2616	16/10/86
41.	Mr S.S. Carter Executive Director Queensland Law Society Inc. GPO Box 1785 BRISBANE QLD 4001	17/10/86
42.	Mr H.T. Bennett Secretary-General Law Council of Australia GPO Box 1989 CANBERRA ACT 2601	22/10/86
43.	The Hon Peter Morris Minister for Aviation Parliament House CANBERRA ACT 2601	20/10/86
44.	Mr D. Murphy Secretary The Australian Society of Labor Lawyers GPO Box 736F MELBOURNE VIC 3001	27/10/86

APPENDIX II

INQUIRY INTO TELECOMMUNICATIONS INTERCEPTION

INDEX OF EXHIBITS

EXHIBIT NO	DESCRIPTION
1.	Exhibit Canberra 25 August 1986, Letter and Document from Mr T.R. Duchesne Registrar, the New South Wales Bar Association dated 28 July 1986.
2.	Exhibit Canberra 25 August 1986, Law Reform Commission of Canada, Working Paper 47, Electronic Surveillance, 1986.
3.	Exhibit Canberra 25 August 1986, Letter from the Office of the Commissioner of the Federal Police, ACT, dated 19 August 1986.
4.	Exhibit Confidential Canberra 25 August 1986.
5.	Exhibit Melbourne 2 September 1986, Extract from "Your Rights" by John Bennett. Attachment to Australian Civil Liberties Union Submission 25 August 1986.
6.	Exhibit Melbourne 2 September 1986, Book "The Wiretapping Problem Today" dated April 1965.
7.	Exhibit Melbourne 2 September 1986, Book "How to Avoid Electronic Eavesdropping and Privacy Invasion".
8.	Exhibit Canberra 18 September 1986, Appendix A to Submission 15; Extract from the Victorian Racing Act 1958.
9.	Exhibit Canberra 18 September 1986, Appendix C to Submission 15; Application Documentation for a Telephone Betting Account.
10.	Exhibit Canberra 18 September 1986, Appendix D to Submission 15; Circuit Diagram for Pip Tone Recorder Connectors.
11.	Exhibit Canberra 18 September 1986, Appendix E to Submission 15; Letter from Telecom dated 2 June 1985.
12.	Exhibit Canberra 18 September 1986, Appendix F to Submission 15; Letter from Telecom dated 11 July 1986 with attachment "Postmaster Generals Press Release dated 31 August 1966"

13. Exhibit Canberra 18 September 1986, Attachment to Submission 15; Tape Recording of a Telephone Betting Transaction.

14. Exhibit Melbourne 29 September 1986, Letter and Attachments from the Assistant Commissioner (Crime) Victorian Police dated 17 September 1986.

14A. Exhibit Confidential, Melbourne 29 September 1986

15. Exhibit Melbourne 29 September 1986, Letter from Telecom Australia to Mr Allatson AFP dated 18 September 1986.

16. Exhibit Sydney 30 September 1986, Letter from Council for Civil Liberties entitled Royal Commission into Alleged Telephone Interception dated 5 May 1986.

17. Exhibit Sydney 30 September 1986, Media Release The New South Wales Bar Association dated 19 May 1986.

18. Exhibit Sydney 30 September 1986, Article entitled Telephone Tapping and Civil Liberties - Satisfying International Obligations by Beverley Schurr, April 1986.

19. Exhibit Sydney 30 September 1986, Newspaper article entitled Choosing the Youth Drug Problem by Claude Forell Melbourne Age 25 June 1986.

20. Exhibit Canberra 24 October 1986, Listening Devices Act, 1984, No. 69 NSW.

21. Exhibit Canberra 24 October 1986, Letter from Graham Hiley, Secretary, Northern Territory Bar Association, dated 15 September 1986.

22. Exhibit Canberra 24 October 1986, Document entitled 'Big Brother Hears You'.

23. Exhibit Canberra 6 November 1986, Documents on Interception of Communications, provided by British High Commission.

24. Exhibit Canberra 6 November 1986, Documents on Interception, provided by the Embassy of the United States of America.

25. Exhibit Canberra 6 November 1986, Documents on Interception, provided by Swedish Embassy.

26. Exhibit Canberra 6 November 1986, Letter dated 23 October 1986 and attachments on Overseas Interception and Listening Devices Legislation and other matters provided by Attorney-General's Department.

27. Exhibit Canberra 6 November 1986, Letter dated 24 October 1986 from the Premier of Western Australia to the Chairman.

28. Exhibit Canberra 13 November 1986, Letter from Mr Justice Stewart, National Crime Authority, dated 7 November 1986.

29. Exhibit Canberra 13 November 1986, Copy of a letter from the Premier of New South Wales to the Prime Minister, forwarded by the Premier's Office, 13 November 1986.

30. Exhibit Canberra 14 November 1986, Letter from the Attorney-General dated 12 November 1986.

31. Exhibit Canberra 18 November 1986, Letter from the Attorney-General's Department dated 17 November 1986.

APPENDIX III

INQUIRY INTO TELECOMMUNICATIONS INTERCEPTION

LIST OF WITNESSES WHO GAVE EVIDENCE AT THE HEARINGSS

WITNESS	DATE OF APPEARANCE AT PUBLIC HEARINGS	TRANSCRIPT PAGE NUMBER
Mr N.S. Reaburn, Senior Assistant Secretary, Security Branch, Attorney General's Department	25/8/86	2
Mr I. Deane, Principal Legal Officer, Security Branch, Attorney General's Department	25/8/86	2
Mr B.C. Bates, Assistant Commissioner, Investigations Department, Australian Federal Police	25/8/86	53
Chief Superintendent P.J. Lamb, Commander Intelligence Division, Australian Federal Police	25/8/86	53
Mr J.T. Bennett, President Australian Civil Liberties Union	2/9/86	152
Mr T. Rippon, General Secretary, Victoria Police Association	2/9/86	199
Mr S.M. Fish, Manager, Communications, Telecom Australia	3/9/86 29/9/86	232 578
Mr W.F. Jamieson, Chief Security Officer, Telecom Australia	3/9/86 29/9/86	232 578
Mr R.L. Orton, Superintending Engineer, Network Management Division, Telecom Australia	3/9/96 29/9/86	232 578
Mr A.K. Wrigley, Director-General of Security, Australian Security and Intelligence Organisation	3/9/86	326

Mr Paul Delianis, Assistant Commissioner, Crime Department, Victoria Police	3/9/86	356
Mr Justice Stewart, Chairman, National Crime Authority	4/9/86	438
Mr D.M. Lenihan, Chief Executive Officer, National Crime Authority	4/9/86	438
Mr G.E. Smith, Senior Adviser, Legal, National Crime Authority	4/9/86	438
Mr J.K. Avery, M.A., Dip Crim, Commissioner of Police New South Wales	4/9/86	505
Executive Chief Superintendent Federick J. Parrington, Officer-in-Charge (Crime), NSW Police Force	4/9/86	505
Detective Superintendent J.F. Foster, Officer-in-Charge,Bureau of Criminal Intelligence, NSW Police Force	4/9/86	505
Superintendent K.J. Drew, Chief of Staff, NSW Police Force	4/9/86	505
Mr John Dowd, M.L.A., President, International Commission of Jurists	4/9/86	546
Mr L.W. Taylor, President, Police Association of NSW	4/9/86	561
Mr B.R. Howe, Secretary, Legal Division, Police Association of NSW	4/9/86	561
Mr J.M. Hartnett, Board Secretary, Totalizator Agency Board of Victoria,	29/9/86	610

Mr D.P. Brignell Assistant General Manager and Director Computer Systems Totalizator Agency Board of Victoria	29/9/86	610
Mr O. Sid Assistant Manager, Telecommunications Totalizator Agency Board of Victoria	29/9/86	610
Mr M.J. Martin Chief of Security Ansett Airlines of Australia	29/9/86	637
Mr T.F. Alton Security Manager Australia Australian Airlines	29/9/86	637
Mr I.M. Musumeci Federal Secretary Australian Telecommunications Employees Association	29/9/86	649
Mr K. Morgan Research Officer Australian Telecommunications Employees Association	29/9/86	649
Ms B. Schurr Committee Member New South Wales Council for Civil Liberties	30/9/86	710
Mr R.V. Hall Journalist/Author 28 Forsyth St GLEBE NSW	30/9/86	837
Mr S.L. Mason Secretary and Director of Research Australian Law Reform Commission	30/9/86	862
Mr R.M. Armstrong Security Manager Australia Qantas Airways Ltd	30/9/86	891
Mr T.A. Game Member of Executive New South Wales Society of Labor Lawyers	30/9/86	899

Mrs T. Cohen Chairman New South Wales Privacy Committee	30/9/86	935
Mr J.W. Nolan Executive Member New South Wales Privacy Committee	30/9/86	935
Ms P.K. Quarry Research Officer New South Wales Privacy Committee	30/9/86	935
Mr T.A.W. Nyman Spokesman Criminal Law The Law Society of New South Wales	30/9/86	1082