TELECOMMUNICATIONS INTERCEPTION AND CRIMINAL INVESTIGATION IN QUEENSLAND: A REPORT

January 1995

ISBN 0-7242-6376-4

Printed by Goprint, Brisbane.

CRIMINAL JUSTICE COMMISSION

Telephone: (07) 360 6060
Facsimile: (07) 360 6333

Your Ref.:
Our Ref.:
Contact Officer:

The Hon. Dean Wells MLA
Minister for Justice and Attorney–General and
Minister for the Arts
Parliament House
George Street
BRISBANE Qld 4000

The Hon. Jim Fouras MLA
Speaker of the Legislative Assembly
Parliament House
George Street
BRISBANE Qld 4000

Mr Ken Davies MLA
Chairman
Parliamentary Criminal Justice Committee
Parliament House
George Street
BRISBANE Qld 4000

Dear Sirs

In accordance with section 26 of the *Criminal Justice Act 1989*, the Commission hereby furnishes to each of you its report on "Telecommunications Interception and Criminal Investigation in Queensland".

Yours faithfully

R. S. O'Regan

R S O'REGAN QC
Chairperson

557 Coronation Drive, Toowong, QLD. 4066, Australia
PO Box 137, Albert Street, Brisbane, QLD. 4002, Australia

FOREWORD

This report considers whether the Queensland Police Service and the Criminal Justice Commission should have the power to intercept telecommunications in certain prescribed circumstances. Mr Fitzgerald QC, in the Report of the Commission of Inquiry (1989), identified this as one of the issues which should be considered in any comprehensive review of powers relevant to law enforcement in Queensland. He also observed that the Commission's Official Misconduct Division was likely to require the power to intercept telecommunications to enable it to discharge its functions effectively.

Under Australia's constitutional arrangements, telephone tapping is governed exclusively by the Commonwealth *Telecommunications (Interception) Act 1979*. For Queensland agencies to have access to this power the State Parliament must pass complementary legislation which complies strictly with the requirements of that Act. There is no latitude to adopt a different arrangement. This means that the only real question for consideration in this report is whether Queensland agencies should participate in the Commonwealth scheme.

The Commission has given close consideration to the law enforcement benefits and cost effectiveness of telephone interception, and to the safeguards and accountability mechanisms contained in the *Telecommunications (Interception) Act*. The conclusion reached is that the capacity of the Commission and the Queensland Police Service to combat organised and major crime will be significantly enhanced by providing them with a strictly regulated power to intercept telecommunications. The Commission is also satisfied that the Act provides an appropriate framework for regulating the use of this power and for protecting legitimate privacy rights.

Some perhaps will argue that the Commission's recommendations may have been conditioned by its operational responsibilities in relation to the investigation of organised and major crime. However, a determined effort has been made to approach the issues dispassionately and to ensure that the information contained in the report is balanced, up-to-date and comprehensive. It is to be hoped that the report will be judged on its merits.

R. S. O'Regan

R S O'REGAN QC
Chairperson

ACKNOWLEDGEMENTS

In preparing this report, officers of the Commission consulted with officers from the Commonwealth Attorney-General's Department, lawyers experienced in the operation of the Commonwealth *(Telecommunications) Interception Act* and the area of electronic surveillance generally, and representatives of various State and Commonwealth police services and investigative agencies. The Commission wishes to acknowledge the valuable assistance provided by these people. The Commission is also grateful to those organisations and individuals who addressed the issue of telephone tapping in written and oral submissions to the Review of Police Powers in Queensland.

Within the Research and Coordination Division, Sonia Caton and Susan Johnson were primarily responsible for researching and writing the report and Tracey Stenzel and Amanda Carter prepared the document for publication. The contributions of all those involved in the project are greatly appreciated by the Commission.

David Brereton
Director
Research and Co-ordination

CONTENTS

ABBREVIATIONS

AFP	Australian Federal Police
ALRC	Australian Law Reform Commission
ASIO	Australian Security Intelligence Organisation
Barrett Review	Review of the Long Term Cost Effectiveness of Telecommunications Interception
Commission	Criminal Justice Commission
Fitzgerald Inquiry	Commission of Inquiry Into Possible Illegal Activities and Associated Police Misconduct
NCA	National Crime Authority
NSWCC	New South Wales Crime Commission
QPS	Queensland Police Service
TID	Telecommunications Interception Division
TIRAC	Telecommunications Interception Remote Authority Connection

CHAPTER 1

INTRODUCTION

PURPOSE OF THE REPORT

This report considers whether the Queensland Police Service (QPS) and the Criminal Justice Commission (Commission) should be given the power to intercept telecommunications in certain prescribed circumstances. This is an important – and controversial – investigative power which is currently not available to either organisation.[1]

The report has been produced pursuant to section 23 of the *Criminal Justice Act 1989*, which defines the Commission's responsibilities to include:

> monitoring and reporting on the use and effectiveness of investigative powers in relation to the administration of criminal justice generally [s. 23(b)]
>
> researching, generating and reporting on proposals for reform of the criminal law and the law and practice relating to enforcement of, or administration of, criminal justice, including assessment of relevant initiatives and systems outside the State [s. 23(e)].

Preparation of the report addresses a recommendation of the Commission of Inquiry Into Possible Illegal Activities and Associated Police Misconduct (Fitzgerald Inquiry) that the power to intercept conversations and communications be considered in any comprehensive review of powers relevant to law enforcement in Queensland (1989, p. 177). The Fitzgerald Inquiry also observed that interception powers were amongst the special powers likely to be required by the Official Misconduct Division of the Commission (1989, p. 313).

THE ISSUES

Under Australia's constitutional arrangements, telecommunications interception, or telephone tapping, is governed exclusively by the Commonwealth *Telecommunications (Interception) Act 1979*. Since 1987 it has been open to State Governments to enact legislation enabling State police services and other investigative bodies to obtain warrants under the Act. However, any complementary State legislation must conform strictly with the requirements of the Commonwealth Act and, in particular, the safeguards which it contains. There is no latitude to adopt a different regime, as the Constitution bestows on the Commonwealth exclusive jurisdiction over this particular activity. To date, New South Wales, Victoria and South Australia have enacted legislation to give law enforcement agencies in those States the power to intercept telecommunications. These agencies now make use of the power on a regular basis (see Figure 2.2).

---

1 The fact that the Commission and the QPS do not have interception powers does not mean that there is no telephone tapping by law enforcement agencies in Queensland. While no data are available, it can be safely assumed that some of the investigations using telephone taps which are undertaken by the Australian Federal Police (AFP) and National Crime Authority (NCA) are directed at criminal activities occurring in Queensland.

In considering whether similar enabling legislation should be enacted in Queensland, this report:

- examines the structure and operation of the *Telecommunications (Interception) Act* to establish whether it provides a suitable framework for regulating the use of telecommunications powers and, in particular, whether it adequately guards against the misuse of these powers and protects privacy rights

- reviews the evidence on the benefits of telephone interception, its cost effectiveness relative to other forms of surveillance, and the justification for, and likely costs of, establishing an interception capability in Queensland.

In preparing this report the Commission has taken the Act as "given", on the grounds that this legislation is the responsibility of the Commonwealth rather than the State. Hence, while critical observations are made where appropriate, the report does not make any recommendations relating to the Commonwealth Act. The report is concerned solely with what action should be taken in Queensland.

BACKGROUND TO THE REPORT

In September 1991 the Commission and the Office of the Minister for Police and Emergency Services, released *Police Powers in Queensland: An Issues Paper*. One matter canvassed in this paper was whether the QPS should be given a power to tap telephones. The Commission subsequently received a number of submissions which included at least some discussion of this issue.

Not surprisingly, the submissions contained a diverse range of views. The QPS, for example, argued strongly that it should have the power to intercept telecommunications in order to effectively discharge its law enforcement role. The QPS stressed that telephone interception was an effective tool in investigating and combating serious crime. The QPS observed that appropriate Commonwealth legislation already existed and that complementary State legislation would have to comply with the minimum standards and safeguards set by the Commonwealth. Numerous other submissions received by the Commission also supported extending telecommunications interception powers to Queensland law enforcement agencies, generally on the proviso that appropriate safeguards would be put in place to prevent abuse of these powers.

On the other hand, several submissions expressed concern about the privacy implications of allowing the QPS to engage in telephone tapping. For example, the Queensland Council for Civil Liberties argued that the extent of telephone interception throughout Australia should be considered before any further extensions of power are granted. Other submissions variously stated that:

- the use of these powers could lead to corruption or could be used on those who oppose the Government

- the safeguards provided under the *Telecommunications (Interception) Act* were inadequate

- the QPS should seek the assistance of Commonwealth law enforcement agencies if it needed to intercept telephones, rather than having powers of its own

- telephone interception simply should not be allowed at either State or Commonwealth level.

The Commission had originally planned to deal with these and related issues in Volume V of its 1994 *Report on a Review of Police Powers in Queensland*, in the context of the issue of electronic

surveillance generally. However, in preparing Volume V it was decided that it would be more appropriate to produce a separate report. As discussed above, in contrast to the other police powers examined by the Commission telecommunications interception is regulated exclusively by the Commonwealth. As such, the question of whether this power should be made available to Queensland law enforcement agencies raises distinct policy and legal issues. Telecommunications interception is also a matter of particular interest to the Commission, given that it has important statutory functions in relation to the investigation of organised and major crime and official corruption. The Commission therefore considered that it should address the question of whether the Commission itself, as well as the QPS, should be able to intercept telecommunications. This could not be easily done in the context of the *Report on a Review of Police Powers in Queensland* as it was concerned exclusively with reviewing powers available to the QPS. A third factor in the Commission's decision to deal with telecommunications interception separately was the knowledge that the Commonwealth planned to introduce significant amendments to the *Telecommunications (Interception) Act* in December 1994 and, at that time, would also be releasing a major report on the operation of the Act (Barrett Review).[2] The Commission was keen to ensure that publication of Volume V was not delayed by the need to wait for the release of this other material, especially as the Parliamentary Criminal Justice Committee had indicated that it wished to hold a public hearing on Volume V well before the end of 1994.

STRUCTURE OF THE REPORT

Chapters Two and Three provide an overview of the development, structure and operation of the *Telecommunications (Interception) Act*.

- Chapter Two outlines the development of telephone interception powers in Australia and presents data on the use of these powers by Commonwealth and State law enforcement agencies.

- Chapter Three describes the major features of the Act, focusing particularly on the safeguards which it contains. Included in this description are the recent proposed amendments contained in the Telecommunications (Interception) Amendment Bill 1994, many of which arose out of the 1994 Barrett Review. Where appropriate, the chapter also draws comparisons between the Act and existing Queensland legislation governing the use of listening devices and other forms of electronic surveillance.

Chapter Four reviews the arguments for giving the QPS and the Commission access to the powers provided under the Act. This chapter considers:

- the law enforcement benefits and cost effectiveness of telephone interception

- the adequacy of the privacy protections and oversight mechanisms contained in the Act

- the desirability of State investigative agencies having direct access to interception powers.

The chapter also presents data on the likely cost of establishing an interception capability in Queensland and discusses other practical and policy matters which will have to be addressed if interception powers are given to the QPS and the Commission.

---

2 *Review of the Long Term Cost Effectiveness of Telecommunications Interception* (1994). The Review is named after its principal author, Mr Pat Barrett, Deputy Secretary of the Commonwealth Department of Finance.

CONCLUSION

The main conclusion of this report is that complementary State legislation should be passed to enable the QPS and the Commission to exercise the powers available under the *Telecommunications (Interception) Act*. This conclusion is based on the Commission's assessment that:

- the capacity of the QPS and the Commission to combat organised and major crime will be enhanced by providing them with the power to intercept telecommunications
- the Act contains adequate mechanisms for protecting privacy and for ensuring that the power to intercept telecommunications is not abused
- telephone intercepts are less intrusive and more cost effective than other electronic surveillance procedures already permitted under Queensland law
- it is impractical and inappropriate for the QPS and the Commission to be dependent upon Commonwealth law enforcement agencies for the exercise of interception powers.

CHAPTER 2

DEVELOPMENT OF TELEPHONE INTERCEPTION POWERS IN AUSTRALIA

INTRODUCTION

Over the last two decades the legislative framework governing telephone interceptions has developed significantly. The legislation has become increasingly complex, adapting to the changing needs of law enforcement and increasing public concerns with privacy protection. The purpose of this chapter is to provide an overview of these developments prior to examining the *Telecommunications (Interception) Act* in detail in Chapter Three. The chapter outlines the evolution of the legislation, summarises the more significant legislative changes and reviews, and presents data on trends in the use of telephone intercepts.

THE INITIAL LEGISLATION

Section 51(v) of the Constitution confers legislative power on the Commonwealth Parliament to make laws with respect to postal, telegraphic, telephonic and other like services. The Commonwealth first invoked this power with respect to telephone interception in 1960, when it passed the *Telephonic Communications (Interception) Act 1960*. Until that time, Prime Ministerial directions given at the end of 1950 governed the use of telephone interceptions. These directions authorised interception only in relation to cases of espionage, sabotage and 'subversive activities' (Commonwealth Attorney-General 1991, p. 1).

The 1960 Act made it an offence to intercept telephonic communications, with the exception of interceptions by officers of the Postmaster-General's Department for technical reasons and interceptions pursuant to warrants issued to the Australian Security Intelligence Organisation (ASIO) in connection with national security matters. The legislation deliberately provided no exceptions for law enforcement purposes. At the time, there was no tangible support for such an extension of powers from either parliamentarians or the public (Australian Law Reform Commission 1983, para. 754 (ALRC); Commonwealth Attorney-General 1991, pp. 1-2).

The 1960 Act was repealed in 1979 and replaced by the Commonwealth *Telecommunications (Interception) Act*. For the first time, this Act permitted a law enforcement body to intercept telephone conversations. The Act, which was passed with bi-partisan support, extended the use of telephone intercepts to the AFP for the investigation of narcotics offences under the *Customs Act 1901* (Commonwealth Attorney-General 1991, p. 3).

RELEVANT REVIEWS AND AMENDMENTS

Interception of telecommunications for law enforcement purposes has been the subject of comment or review in a number of major inquiries undertaken in the 1980s and 1990s. These have included:

- Australian Royal Commission of Inquiry Into Drugs 1980 (Williams Commission)
- *Royal Commission of Inquiry Into Drug Trafficking* 1983 (Stewart Commission)

- Australian Law Reform Commission 1983, *Privacy* (ALRC)
- *Royal Commission Into Alleged Telephone Interceptions* 1986 (Stewart Commission)
- *Review of the Telecommunications (Interception) Act 1979* (Commonwealth Attorney-General 1991)
- Barrett Review 1994.

ROYAL COMMISSIONS

The 1981 Williams and 1983 Stewart Royal Commissions focused on telecommunications interception in relation to the investigation of drug offences.

The report of the Williams Commission was handed down after the 1979 *Telecommunications (Interception) Act* had been passed but before it became operative. The scheme recommended by Williams J 'was clearly part of a more considered and all embracing policy approach to the issue of drug crime detection than that embodied in the 1979 Act' (Barrett Review 1994, p. 49).[3] However, the scheme was not adopted, probably because it was proposed too soon after Parliament had enacted the Act (Barrett Review 1994, p. 49).

In 1983 the report of the Stewart Commission on drug trafficking was published. Stewart J agreed broadly with the recommendations of Williams J. Notable among the recommendations of Stewart were that interception powers should be available for narcotics offences and other 'organised crimes' and that the powers should be extended to State police.

The findings of the Williams and Stewart Commissions prompted a Special Premiers' Conference on drugs in 1985. There, the Commonwealth announced its willingness to make interception powers available to State police services if requested by the Governments of the States (Barrett Review 1994, p. 53).

In 1986 the Stewart Commission on alleged telephone interceptions reported disturbing information about the extent of illegal interception by the New South Wales Police Service. However, Stewart J found that these illegal interceptions had produced valuable criminal intelligence. Ultimately, the Stewart Commission recommended the expansion of telephone interception powers to a broader range of offences and to State police services and the NCA.

[3] For a more detailed discussion see Australian Royal Commission of Inquiry Into Drugs 1980, *Report: Outlines of Recommended Uniform Legislation*, Book F, (Commissioner: The Hon. Mr Justice E. S. Williams), AGPS, Canberra, pp. F21-F23.

THE AUSTRALIAN LAW REFORM COMMISSION

The ALRC's 1983 report on privacy provided a timely focus on the concerns associated with telephone interception. The ALRC accepted that there were circumstances in which the social benefits flowing from police use of interception could outweigh the cost, in privacy terms, to individuals subjected to the use of such techniques (ALRC 1983, vol. 2, p. 61). However, the ALRC also pointed out that privacy concerns could sometimes be given insufficient weight in the political decision-making process:

> . . . in any particular case, the arguments for engaging in data surveillance are likely to be considered more immediate and compelling than what may appear to be the more absolute and philosophical concerns underlying information privacy interests (ALRC 1983, vol. 1, p. 20: citing Commission on Freedom of Information and Individual Privacy, Ontario, Public Government for Private People, vol. 3, 1980, p. 505).

The ALRC criticised the 1979 Act, expressing concern that accountability provisions such as public reporting requirements were not included in the Act. The ALRC was also concerned that the extension of interception powers to narcotics offences would lead to increasing demands by the AFP and other law enforcement agencies for further extensions of the power to cover other problem areas and law enforcement generally. The ALRC made several criticisms of the scheme, including:

- there was no express requirement that the judge consider whether the use of other investigative procedures was more appropriate
- the warrant did not need to specify the offence, persons and places that were to be the subject of surveillance
- the applicant for a warrant did not have to support his or her application with an affidavit
- the warrant could remain in force for up to six months
- there was no mechanism for publicly reporting the extent of telecommunications interception (1983, pp. 355–357).

Most of these concerns have since been addressed, to varying degrees, by amendments to the Act.

THE 1987 AMENDMENTS

In 1986 the Commonwealth prepared a Bill providing, among other things, that in certain circumstances the NCA and State law enforcement agencies could use telephone interception powers. A Parliamentary Joint Select Committee[4] examined the Bill and, following its report, a modified version was introduced into Parliament and passed in 1987. Consistent with a recommendation of the Select Committee, the revised Bill extended the range of offences for which warrants could be sought to include, for example, other serious drug offences, murder, kidnapping and serious fraud.

The Select Committee considered the central co-ordination of interception to be an important safeguard. The 1987 amendments required all warrants to be executed by the newly created

[4] This was the first Joint Select Committee to examine a Bill originating in the House of Representatives. It was established because the Government believed that the question of an extension of interception powers called for thorough parliamentary consideration (Commonwealth Attorney-General 1991, p. 7).

Telecommunications Interception Division (TID) of the AFP, including warrants granted to State agencies under any State legislation. The TID was to record intercepted communications and transmit them simultaneously to the relevant law enforcement agency (Commonwealth Attorney-General 1993, p. 7). This centralisation of the execution of warrants was seen by the Privacy Commissioner as 'a means of guarding against the undue intrusion into privacy arising from having a proliferation of law enforcement bodies carry[ing] out the activity' (Human Rights and Equal Opportunity Commission 1992, p. 1). The 1987 Act also included provisions requiring agencies to keep detailed records relating to interceptions, make these records available to an Ombudsman-type body, and satisfy various annual reporting requirements.

Since the 1987 amendments, the NCA, Victoria Police, New South Wales Police Service, New South Wales Crime Commission (NSWCC), Independent Commission Against Corruption and South Australian Police Service have each been granted the power to intercept telecommunications. Table 2.1 shows when this power was conferred.

TABLE 2.1 – CONFERMENT OF TELECOMMUNICATIONS INTERCEPTION POWER ON STATE AGENCIES

Agency	Date
Victoria Police	28 October 1988
New South Wales Crime Commission	30 January 1989
New South Wales Police Service	30 January 1989
New South Wales Independent Commission Against Corruption	6 June 1990
South Australian Police Service	10 July 1990

Source: Commonwealth Attorney-General 1993, p. 5

THE 1991 REVIEW BY THE ATTORNEY-GENERAL'S DEPARTMENT AND THE 1993 AMENDMENTS

When introducing the 1987 amendments, the Commonwealth agreed to review the operation of the legislation two years after implementation. The review was carried out by the Attorney-General's Department which reported in December 1991 following extensive consultation. As a result of that review, the Act was further amended in 1993. The main changes introduced were:

- limited provision for emergency interceptions subject to later authorisation by the court [ss. 7(4) – (11)]

- the inclusion of computer related offences in the offences for which a warrant could be sought

- the replacement of the centralised execution of warrants system (TID) by the Telecommunications Interception Remote Authority Connection system (TIRAC).

A joint submission to the Attorney-General's Department by all State and Commonwealth law enforcement agencies, other than the AFP, argued for the devolution of the interception function to each agency. The problems which agencies raised in relation to the TID system included delay, unfamiliarity of AFP members with individual investigations, security, technical difficulties and costs. The review team was reluctant to replace the TID but ultimately recommended adoption of the TIRAC system. This system involves the installation of a computer link-up between the TID in Canberra and each agency, enabling the interception to be made at the agency but under the control of the AFP (Commonwealth Attorney-General 1991, pp. 28-33).

THE BARRETT REVIEW AND THE 1994 BILL

In 1993, the Commonwealth initiated a comprehensive review of the *Telecommunications (Interception) Act*, focusing on the long term cost effectiveness of telecommunications interception. The Barrett Review 1994 was released at the same time as the introduction of the Telecommunications (Interception) Amendment Bill 1994 into the Senate.

Barrett's terms of reference required him to assess:

- Australia's telecommunications interception capability
- the need for an interception capability for criminal investigations, prosecutions and security interests
- measures to safeguard privacy and the effectiveness of the present scheme in protecting individual privacy from unlawful and unwarranted interceptions
- the benefits of telecommunications interception both within Australia and overseas.

The main findings of the review were:

- telecommunications interception can be a very cost effective investigative technique, particularly as a complement to other methods of investigation and intelligence gathering (in the case of security agencies)
- the way in which telecommunications interception is being conducted in Australia is consistent with the requirements of the Act, particularly in regard to privacy considerations
- more privacy focused inspections and greater transparency through notification procedures and additional reporting would further enhance privacy
- due to recent technical developments there has been, and will continue to be, degradation of telecommunications interception capability which can be overcome for the next three to five years at 'not insignificant cost'.[5]

[5] The Barrett Review offers the most detailed consideration to date of the more technical issues which are currently affecting the cost of interception. Some of its findings in this respect are discussed later in this chapter.

Barrett found that there was insufficient information available to make a projection about the telecommunications industry beyond 1997, when the industry will be fully deregulated. He therefore recommended that a further review be carried out in that year, as it would permit a much better understanding of the likely market and 'the requirements for, and difficulties with, interception in such an environment' (Barrett Review 1994, pp. 4–5).

Recommendations by Barrett which have been incorporated into the 1994 Telecommunications (Interception) Amendment Bill include:

- the offences for which a warrant can be sought be expanded to include more serious offences involving corruption or organised crime and money laundering (Recommendation 2)
- a civil right of action be available to a person whose communication is unlawfully intercepted (Recommendation 8)
- agencies' reporting obligations be extended to include the average cost of each interception and a general indication of the proportion of warrants yielding information used in the prosecution of an offence (Recommendation 12)
- agencies' reports on the execution of particular warrants include an assessment as to how useful the information was and whether it led to an arrest or was likely to do so (Recommendation 13).

Only two of Barrett's recommendations have not been adopted. The Commonwealth Government has rejected Barrett's proposal that the inspection and reporting function currently carried out by the Commonwealth Ombudsman be transferred to the Privacy Commissioner (Recommendation 6). The Government has also not accepted Barrett's recommendation that agencies be required to notify any innocent person whose telephone service has been intercepted of the fact of the interception within 90 days of the cessation of the interception (Recommendation 7). However, a fallback position proposed by Barrett has been accepted. Under this arrangement, agencies will be required to maintain a register of incidents where the telephone service of an innocent person has been intercepted. The register is to be made available to the relevant inspecting agency for inspection and report to the Attorney-General.

THE USE OF TELECOMMUNICATIONS INTERCEPTION POWERS

The number of telecommunication interception warrants issued by the courts for law enforcement purposes has steadily climbed in recent years. Between 1988/89[6] and 1993/94, the number of warrants issued increased from 246 to 668 – a rise of 170 per cent (Figure 2.1). This increase has been due partly to State agencies being authorised to apply for warrants. As shown by Figure 2.2, State agencies now account for slightly under half of all warrants issued. However, the increase in the number of warrants is not simply due to more agencies being given interception powers. Within most agencies there has also been an increase in the use of this facility. For instance, the number of warrants issued to the AFP rose from 188 in 1990/91 to 287 in 1993/94.

6 1988/89 was the first year for which an annual report was produced on the operation of the *Telecommunications (Interception) Act*. Data are not available on the number of warrants issued in the years prior to then. The Annual Report does not contain any details on warrants issued to ASIO.

Other factors relevant to the increase in use include:

- more lines becoming available for interception and more agency resources being dedicated to interception, because of the effectiveness of this form of surveillance (see Chapter Four)
- the increasing sophistication of organised criminal activity requiring more refined approaches
- an increase in the number of offences for which warrants may be obtained.

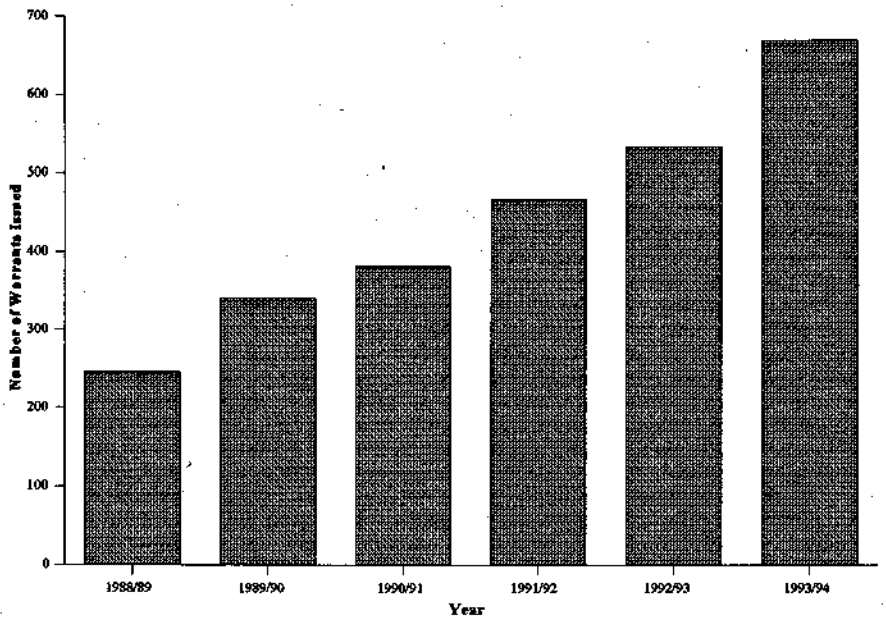

FIGURE 2.1 – TELECOMMUNICATIONS INTERCEPTION WARRANTS ISSUED AUSTRALIA 1988/89 – 1993/94

Source: Commonwealth Attorney-General; unpub. data for 1993/94.

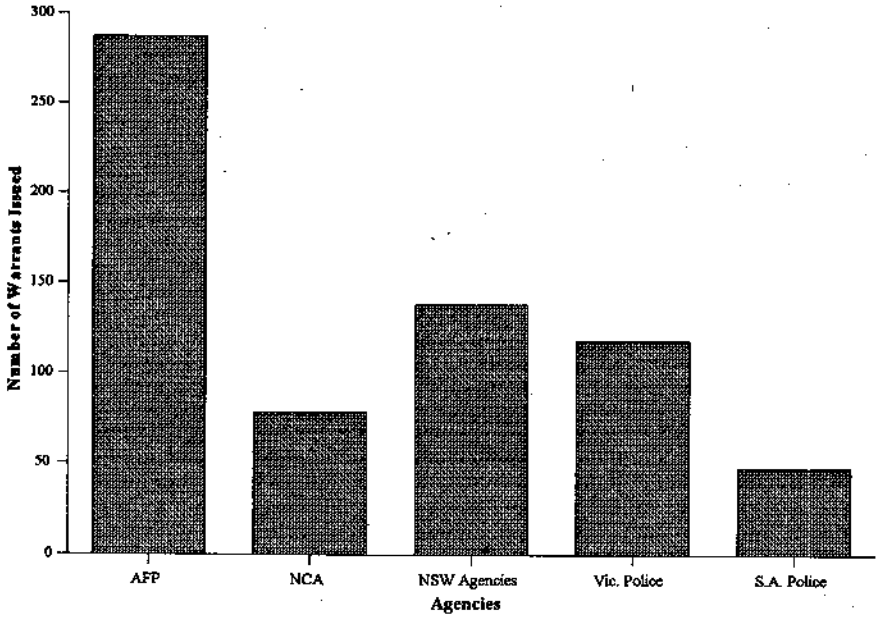

FIGURE 2.2 – BREAKDOWN OF WARRANTS ISSUED BY AGENCIES 1993/94

Source: Data provided by Commonwealth Attorney-General's Department.

Note: 'NSW agencies' encompasses the NSW Police, NSWCC and the Independent Commission Against Corruption.

The majority of warrants continue to be issued in relation to drug offences, but there has been an increasing issue of telephone intercepts to investigate other types of offences, particularly murder and serious fraud. In 1993/94, warrants relating to drug trafficking offences and narcotics offences under the *Customs Act 1901* constituted 56 per cent of all warrants issued. This proportion has fallen considerably from 1988/89 when warrants relating to such offences accounted for 84 per cent of all warrants. Conversely, there has been an increase in the number of warrants issued in relation to serious crimes against the person and serious fraud.

As discussed in detail in Chapter Four, there has been a very high "success rate" in investigations which use telephone interceptions. For instance, data published in the 1992/93 annual report show that in that year 434 convictions were secured from prosecutions which relied wholly or partly on intercepted communications.

Although telecommunications interception will continue to be an important investigative tool in the short to medium term, the capability of this technique is coming under increasing challenge. This is largely due to the unregulated release of new communication technologies, which are not easily intercepted, onto the domestic market. These developments have also contributed to the rising costs of telecommunications interception. Digital telephony and encryption have been identified as the biggest current threats to interception in the United States and Canada (Barrett Review 1994, p. 4). These technologies are not quite so established in Australia, but time will see their increasing use.

CONCLUSION

Since 1960 there have been several reviews of, and modifications to, telecommunications interception legislation in Australia. One effect of these changes has been to substantially expand the circumstances in which interceptions can be lawfully undertaken by:

- widening the range of offences for which interception warrants can be sought, to include serious crimes other than drug-related offences

- extending the power to obtain warrants to State law enforcement agencies.

These legislative changes, in conjunction with the increased investment of resources by law enforcement agencies at both State and Commonwealth level, have resulted in a very substantial increase in the number of interception warrants being issued by the courts.

It is important to emphasise, however, that the growth in the availability and use of telecommunications interception powers has been parallelled by an increase in the level of accountability and privacy protection provided under the *Telecommunications (Interception) Act.* The Act has been reviewed much more regularly and critically than any State legislation dealing with other forms of electronic surveillance. As a consequence, it now contains substantially more comprehensive privacy and accountability provisions than can be found at State level. The following chapter looks in some detail at these provisions, in the context of a general account of the scope and regulation of interception powers under the Act.

CHAPTER 3

THE STRUCTURE AND OPERATION OF THE *TELECOMMUNICATIONS (INTERCEPTION) ACT 1979*

INTRODUCTION

Before telephone interception powers could be conferred on the QPS or the Commission the Queensland Parliament would have to enact legislation which conforms with the requirements of the *Telecommunications (Interception) Act*. In considering whether Queensland should take this action, it is essential to understand the way in which the Act operates, the requirements which it sets down for State legislation and the safeguards which it imposes.

This chapter outlines the main features of the Act under the following headings:

- the general framework of the Act
- obtaining access to telecommunication interception powers
- offences for which warrants may be sought
- application procedures
- matters a judge is to consider in issuing a warrant
- length of warrants
- revocation of warrants
- dealing with intercepted information
- criminal offences and civil remedies
- record-keeping and reporting requirements
- oversight by an independent agency.

This chapter includes reference to the proposed amendments to the Act that are currently before the Commonwealth Parliament. The chapter also compares aspects of the Act with Queensland legislation governing other forms of electronic surveillance (in particular the *Invasion of Privacy Act 1971*) and, where appropriate, with the Commission's recommendations in Volume V of the *Report on a Review of Police Powers in Queensland: Electronic Surveillance and Other Investigative Procedures*.[7]

[7] Tables summarising the key features of Queensland listening device legislation and the Commonwealth *Telecommunications (Interception) Act* are contained in Appendix 14 of Volume V.

GENERAL FRAMEWORK OF THE *TELECOMMUNICATIONS (INTERCEPTIONS) ACT*

The Act has two main purposes (Commonwealth Attorney–General 1993, p. 4):

- to protect the privacy of individuals who use the Australian telecommunications system
- to specify the circumstances under which it is lawful for an interception to take place.

The Act prohibits a person from intercepting a communication passing over the telecommunications system except where permitted by the Act (s. 7). Generally, interception is only lawful where it is made in connection with the operation or maintenance of the telecommunications system or, most importantly, with the authority of a warrant.

The provisions of the Act deal with matters such as: which organisations are eligible to obtain warrants; the offences for which warrants may be obtained; procedures for applying for, issuing, executing and revoking warrants; the use of information obtained under warrants; and the penalties and remedies which apply when the provisions of the Act are breached. In addition, the Act subjects agencies to detailed record–keeping and reporting requirements and provides for independent oversight of their activities.

OBTAINING ACCESS TO TELECOMMUNICATIONS INTERCEPTION POWERS

For a State police service or investigative body to be able to intercept telecommunications, three requirements must be met:

- The organisation must have been designated as an 'eligible authority' of a State or Territory under the *Telecommunications (Interception) Act*. Both the QPS and the Commission are eligible authorities for this purpose.[8]
- The relevant State Government must have introduced complementary legislation which complies with the requirements contained in section 35 of the Act. The State legislation must require the chief officer of any 'eligible authority' to conform with record–keeping and reporting requirements similar to those which apply to Commonwealth law enforcement agencies under the Act. In addition, the legislation must designate an appropriately resourced independent authority with the same powers of inspection as are exercised by the Commonwealth Ombudsman in relation to the AFP and NCA.
- The Premier of the State concerned must have requested the Commonwealth Attorney–General to declare the organisation an 'agency' for the purposes of the Act and the Attorney–General must have acceded to that request [s. 34(1)].

The Commonwealth Attorney–General may revoke a declaration at the request of the State Premier or on his or her own initiative if satisfied that the State legislation does not meet the requirements of

[8] Under s. 5, 'eligible authority' includes any State or Territory police force. The Commission was included in the list of eligible authorities by the *Telecommunications (Interception) Amendment Act 1993*. Designation as an 'eligible authority' means that the organisation concerned is able to receive intercepted information.

the Act, or if there is inadequate compliance by the agency with the provisions of the State legislation (s. 37).

OFFENCES FOR WHICH WARRANTS MAY BE SOUGHT

The *Telecommunications (Interception) Act* provides a comprehensive list of the range of offences for which interception warrants may be obtained. The Act designates two classes of offence. Class 1 offences include murder, kidnapping, serious narcotics offences under the *Customs Act 1901* (Cwlth) and aiding, being concerned in or conspiring to commit those offences.[9] Class 2 offences include offences against a provision of Part VIA of the *Crimes Act 1914* (Cwlth) and offences for which a penalty of seven years imprisonment or more can be imposed, where the conduct involves:

- loss or serious risk of loss of a person's life
- serious personal injury or serious risk of such injury
- serious damage to property endangering personal safety
- trafficking in narcotic drugs or psychotropic substances
- serious fraud
- serious loss to the revenue of the Commonwealth or of a State
- aiding, being concerned in, or conspiring to commit any of these offences.

Amendments currently before Commonwealth Parliament[10] will extend class 2 offences to include money-laundering, corruption and organised crime. Under the proposed amendments organised crime is defined as an offence for which a penalty of seven years imprisonment or more can be imposed, where the conduct:

- involves two or more offenders and substantial planning and organisation
- involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques
- is committed, or is of a kind that is ordinarily committed, in conjunction with other offences of a like kind
- consists of, or involves, any of the following:
  - ⋆ theft
  - ⋆ handling of stolen goods
  - ⋆ tax evasion

9 For the purposes of the NCA, class 1 offences also include offences in relation to which the NCA is conducting a special investigation.

10 Telecommunications (Interception) Amendment Bill 1994.

- currency violations
- extortion
- bribery or corruption of an officer of the Commonwealth, a State or a Territory
- bankruptcy violations
- company violations
- harbouring criminals
- armament dealings
- a sexual offence against a person under 16 (including offences against Part IIIA of the *Crimes Act 1914*).

These amendments are consistent with the recommendations of the Barrett Review. Barrett proposed the extension of offences to organised crime and corruption, referring to the findings of the Commonwealth's Review of Law Enforcement Arrangements 1994. The report of this review described the increasing costs of white collar crime and the growth in organised crime being considerably assisted by corruption in key areas of the economy and governmental institutions. Barrett was also concerned to ensure that the Act did not exclude more serious offences than those already included in class 2 (Barrett Review 1994, p. 33).

The Commission, in Volume V of its Police Powers report, recommended that a similar classification of offences to that outlined above should be incorporated into Queensland listening device legislation. Currently, the *Invasion of Privacy Act* theoretically allows an application for a listening device warrant to be made in relation to any offence (Commission 1994, pp. 758–759).

APPLICATION PROCEDURES

Applications for telephone interception warrants, whether sought by a Commonwealth or State law enforcement agency, can only be made to a Federal Court judge.

The application must be made in writing unless there are urgent circumstances which justify a telephone application (see below).

The Act sets down in detail the matters which must be addressed in a warrant application. The application must state the name of the agency and the name of the person making the application on the agency's behalf, and must be accompanied by an affidavit (ss. 41 and 42). A supporting affidavit must contain the following information:

- the facts and other grounds on which the application is based
- the period for which it is requested that the warrant be in force
- the reasons why it is considered necessary for the warrant to be in force for that period of time
- the number of previous applications (if any) for warrants that the agency has made that relate to the telephone service or to the person who is the target of the application

- the number of warrants (if any) previously issued on such applications
- particulars of the use made by the agency of information obtained by interceptions under such warrants.

A judge may require further information to be given on oath (s. 44).

These provisions compare very favourably with current Queensland listening device legislation which does not specify application procedures to be followed or the matters to be addressed in warrants (Commission 1994, pp. 784–788).

ENTRY ONTO PREMISES

The judge may authorise entry onto premises for the purpose of installing, maintaining, using or recovering interception equipment if he or she is satisfied that it is impractical to intercept the service without installing the equipment (s. 48). Entry onto premises may be necessary for technical reasons associated with the nature or operation of the particular target service or telecommunications system; or because the security of the operation might otherwise be jeopardised.

If authority to enter premises is sought, the application must specify the premises, and be supported by an affidavit setting out:

- the reasons why it is considered necessary for the warrant to authorise entry
- the number of previous applications (if any) for warrants that the agency has made requesting authorisation of entry on those premises
- the number of warrants (if any) previously issued on such applications.

In practice, because of the nature of the technology employed, entry onto premises is rarely necessary to effect interception – in 1992/93 only three of the 553 applications for interception warrants sought such an authority (Commonwealth Attorney–General 1993, p. 18). By contrast, in virtually all cases where a warrant for a listening device is issued, entry to the premises is required in order to install and retrieve the device.

URGENT APPLICATIONS

Section 40(2) provides that in urgent circumstances applications for warrants may be made by telephone. Such applications must be accompanied by an explanation of the circumstances of urgency and followed by an affidavit similar to that submitted for applications in the normal course (ss. 43 and 51). If a judge is satisfied that certain procedures applying to telephone warrants have not been complied with, he or she may revoke such warrants under the provisions of section 52. Five telephone applications were made in 1992/93 (Commonwealth Attorney–General 1993, p. 16) representing around one per cent of all applications.

Amendments[11] made in 1993 authorise interception by the AFP and State police services without a warrant in certain urgent circumstances [s. 7(4) and (5)]. Amongst other restrictions, this power can

11 See s. 10 of the *Telecommunications (Interception) Amendment Act 1993.*

only be exercised where the officer of the agency concerned is a party to the communication, or the person to whom the communication is directed has consented to the interception. In all such cases, an application is to be made for a warrant as soon as practicable after the interception [s. 7(6)].

MATTERS A JUDGE IS TO CONSIDER IN ISSUING A WARRANT

In relation to class 1 offences (see above), the matters the judge must consider when determining whether or not to issue a warrant include whether (s. 45):

- there are reasonable grounds for suspecting that a particular person is using, or likely to use, the telecommunications service
- the information likely to be obtained by the interceptions would be likely to assist the applicant agency in the investigation of the offence or offences in which the person is involved
- some or all of the information cannot appropriately be obtained by other methods that do not involve the interception of communications, having regard to:
    - ⋆ the extent to which such other methods of investigation have been used or are available to the agency
    - ⋆ how much of the information sought would be likely to be obtained using such methods
    - ⋆ how much the use of such methods would be likely to prejudice the investigation, because of delay or any other reason.

In relation to class 2 offences a judge must also consider:

- how much the privacy of any person or persons is likely to be interfered with by the interception and
- the gravity of the conduct constituting the offence or offences being investigated (s. 46).

The fact that a judge is not required to consider the privacy of the subject of the surveillance in relation to class 1 offences has been a matter of some controversy. No such distinction is made in Queensland legislation governing listening devices. In other respects, however, this legislation compares unfavourably with the provisions of the *Telecommunications (Interception) Act*, as there is no requirement for Queensland courts to consider whether the evidence sought to be obtained from a listening device could be obtained by other, less intrusive means (Commission 1994, pp. 763–766).

Figures provided in the annual reports on the operation of the Act show that, on average, less than one per cent of applications are refused. However, this does not mean that warrants are easily obtained. Arguably, because the process is very rigorous, agencies do not apply for warrants unless there is a strong chance of success. According to the Barrett Review, Federal Court judges were highly commendatory of the thoroughness of the warrants and the care taken by the agencies (1994, p. 56).

The proportion of warrants that are issued with conditions or restrictions has increased slightly from 1.5 per cent in 1991/92 to 4.6 per cent in 1992/93 (Commonwealth Attorney-General 1993, p. 19).

LENGTH OF A WARRANT

Under the Act the judge may issue a warrant enforceable for up to 90 days (s. 49). However, where the Chief Officer of an agency to which a warrant has been issued is satisfied that the grounds on which the warrant was issued have ceased to exist, he or she is required to revoke the warrant (ss. 56 and 57). In 1992/93 the average specified length for warrants issued under the Act was 80.2 days, although warrants were actually only in force for an average of 45.7 days (Commonwealth Attorney–General 1993, p. 25).

Section 49(4) provides that a judge shall not vary a warrant by extending the period for which it is to be in force. Instead, the Act requires that a fresh application be brought for a new warrant to be issued upon the expiry of an existing warrant. This ensures periodic judicial review of extended interception operations.

In 1992/93, 82 applications were made for renewal warrants and all were granted. Nearly three quarters of those were made by Commonwealth agencies. The average period specified in renewal warrants was 82.2 days and the average period these warrants were in force was 52.2 days (Commonwealth Attorney–General 1993, p. 25).

Queensland listening device legislation does not specify a maximum time limit, although current practice is for courts to issue warrants for a maximum of 28 days. The Commission has recommended that this standard be incorporated into legislation with provision for extension of a further 28 days. The Commission's view is that strict time limits should be imposed in relation to listening device warrants, due to the particularly intrusive nature of this form of surveillance (Commission 1994, pp. 782–783).

DEALING WITH INTERCEPTED INFORMATION

Information obtained through an interception is not allowed to be communicated, made use of, recorded or given in evidence except as permitted by Part VII of the Act (s. 63). The provisions of the Act relate both to lawfully and unlawfully obtained information.

LAWFULLY OBTAINED INFORMATION

Broadly, officers of agencies may communicate lawfully obtained information to another person (s. 68):

- for the investigation of prescribed offences,[12] or
- if the information relates to the possible commission of any 'relevant offence'.[13]

---

12 'Prescribed offence' is defined in s. 5 to include a serious offence (that is, a class 1 or class 2 offence); certain offences under the Act; an offence against a provision of the Part VIIB of the *Crimes Act 1914*; any other offence punishable by imprisonment for life or for a period, or maximum period, of at least three years; or an offence ancillary to the above offences.

13 Section 5 defines 'relevant offence' to include a 'prescribed offence' that is an offence against a law of the Commonwealth; a prescribed offence that is an offence against a law of the State; or a prescribed offence that is an offence over which the agencies have jurisdiction.

A member of the police service may communicate information received as the result of an emergency trace under section 30 to any person whose assistance may be required in dealing with that emergency (s. 70).

Employees of a carrier,[14] in performance of their duties, may communicate information relating to:

- the operation or maintenance of the network operated by the carrier or supply of the services by the carrier or another by means of the network (s. 63B)
- the investigation by an agency of a serious offence (s. 65A).

A person who has intercepted a communication pursuant to a warrant may communicate that information to an officer who applied for the warrant or who is authorised to receive such information (s. 66).

Lawfully obtained information is not to be used as evidence except in 'exempt proceedings' (s. 74; s. 77).[15] These are defined in section 5B to include proceedings:

- by way of a prosecution for a prescribed offence
- for the confiscation or forfeiture of property or the imposition of a pecuniary penalty in connection with the commission of the prescribed offence
- for extradition relating to a prescribed offence
- in relation to police discipline
- in relation to alleged misbehaviour or improper conduct of an officer of the Commonwealth or a State
- for recovery of a debt due in relation to supply of a telecommunications service
- that concern an offence against the laws of a foreign country punishable by imprisonment for life or for a period, or maximum period, of at least three years.[16]

In 1992/93, lawfully obtained evidence was given in 538 prosecutions for prescribed offences. The great majority of these prosecutions related to drug offences (Commonwealth Attorney-General 1993, p. 30).

---

14 A carrier is a provider of telecommunications services, for example Telecom, Optus or Vodaphone.

15 A person may communicate to another person, or give in evidence in a proceeding, information obtained by interception for the purpose of a determination being made of the extent, if any, to which s. 74 (and other provisions of the Act) permits a person to give that information in evidence in the proceedings [s. 77(1)(b)].

16 Pursuant to s. 13 of the *Mutual Assistance in Criminal Matters Act 1987.*

UNLAWFULLY OBTAINED INFORMATION

Unlawfully obtained information cannot be communicated or used in evidence in proceedings unless it:

- is for the purpose of a proceeding begun prior to the commencement of Part VII of the Act (September 1988) and was obtained prior to that date [s. 63A, s. 77(1)(a)]; or
- has been communicated to the Commonwealth Attorney–General, the Commonwealth Director of Public Prosecutions, the AFP Commissioner or the NCA chairperson by a person who suspects on reasonable grounds that the interception may tend to establish a breach of the Act (s. 71); or
- is given in evidence in a proceeding for a prosecution for a breach of the Act (s. 76).

Overall, the effect of the various provisions of the Act relating to the disclosure of lawful and unlawful information is to strictly limit the circumstances in which intercepted information can be used. Broadly speaking, these constitute legitimate law enforcement purposes.

CRIMINAL OFFENCES AND CIVIL REMEDIES

As noted earlier, a major objective of the Act is to prohibit the unauthorised interception of communications passing over the telecommunications system. To assist in enforcing this prohibition the Act creates an offence punishable by two years imprisonment for contravening the prohibitions against interception and the restrictions upon communication of lawfully obtained information.

Until recently there were no civil remedies available to a person whose communication was unlawfully intercepted. The Barrett Review recommended that a right of action be conferred on that person (Recommendation 8) as a means of enhancing privacy protection. That recommendation has been adopted by the Government and is reflected in the 1994 Bill. The relevant provision states that an 'aggrieved person' may bring an action in court seeking remedial relief against a person who intercepted a communication in breach of the Act or who communicated information in contravention of the Act (see cl. 107A). An 'aggrieved person' is defined as a party to the intercepted communication or on whose behalf the intercepted communication was made. The Bill provides for both civil and criminal courts to make such orders in particular circumstances. The kinds of orders that the court would be able to make under this provision include:

- an order declaring that the interception was unlawful
- an order that the defendant pay damages to the aggrieved person
- an injunction
- an order that the defendant pay the aggrieved person an amount not exceeding the total gross income derived by the defendant as a result of the interception or communication.

There is no equivalent provision in the State listening device legislation.

RECORD-KEEPING AND REPORTING REQUIREMENTS

The Act has a comprehensive scheme for recording and reporting upon its operation. An integral part of the scheme is the independent oversight of agency records by the Ombudsman or, at State level, some similar authority. There are currently no equivalent requirements in Queensland legislation governing listening devices even though it is generally accepted that listening devices are a more intrusive form of surveillance (Commission 1994, pp. 798–814).

RECORD-KEEPING REQUIREMENTS

Under the Act, Commonwealth and State agencies must retain comprehensive records of specified information regarding each warrant application. This information includes (ss. 80–81):

- particulars of telephone applications
- whether each application was refused or withdrawn, or a warrant issued
- particulars of the warrant, day and time of each interception and name of the person who carried out such interception
- communication of restricted records
- uses of 'lawfully obtained information'
- the giving in evidence of lawfully obtained information.

Amendments to the Act in 1993 also require the Commissioner of the AFP to keep a register of warrants issued to all agencies. The register must include the following information in relation to each warrant (s. 81A):

- the date of issue and the judge who issued it
- the agency to which it was issued
- the telecommunications service to which it relates
- the name of the person specified in the warrant as the person likely to use the service
- the period for which the warrant is to be in force
- each serious offence of which the judge issuing the warrant was satisfied on the application for the warrant.

The Commissioner is required to provide an up-dated register to the Commonwealth Attorney-General every three months for inspection.

The 1994 Bill includes a requirement to keep a special register of incidents where the telephone service of an innocent person has been intercepted. That register is also to be made available to the Commonwealth Attorney-General for inspection every three months. As noted in Chapter Two,

Barrett's preferred approach was for innocent persons to be notified that their conversations had been intercepted, but this recommendation was not accepted by the Government.[17]

REPORTS TO THE COMMONWEALTH ATTORNEY-GENERAL

Chief officers of Commonwealth agencies must provide the Attorney-General with copies of all warrants, reports on the use made by the agency of intercepted information and comprehensive reports on the matters the Minister must address in an annual report to Parliament (s. 94). 'Declared' State and Territory eligible authorities that can access powers under the Act must be subject to similar reporting requirements under their own legislation. State and Territory eligible authorities must also provide the Commonwealth Attorney-General with comprehensive yearly reports (s. 96).

The reports must contain information relating to the effectiveness of warrants, including how many arrests, prosecutions and convictions were made during that year on the basis of information that was lawfully obtained by the use of interception devices. The following information must also be provided:

- the number of applications made and warrants issued
- the average periods specified in warrants that were issued
- the average period of time for which warrants were sought
- the number of renewals of warrants that were sought and granted
- the average length of time of such renewals
- other details in relation to the class and nature of offences for which warrants were sought
- the number of interceptions without warrants
- total expenditure (including capital expenditure) incurred by agencies in connection with the execution of warrants.

In addition, the Managing Directors of carriers (e.g. Telecom, Optus) must provide reports to the Attorney-General on acts or things done in relation to warrants (s. 97).

ANNUAL REPORT TO PARLIAMENT

Under Divisions 2 and 3 of Part IX of the Act, the Commonwealth Attorney-General is required to table a comprehensive annual report in Commonwealth Parliament in relation to the use of interception devices by both Commonwealth and State agencies. The report contains the information that the agencies are required to provide to the Minister (see above).

---

17 In Volume V of its Police Powers report, the Commission recommended that the judge who issued a warrant to install a listening device be given the discretion to notify a person that he or she had been the subject of surveillance. It was the Commission's view that this discretion should be exercisable in relation both to those persons deemed 'innocent' and those who were to be charged as a result of the investigation (Commission 1994, pp. 809-811).

The 1994 Bill contains a provision requiring annual reports to provide a general indication of the proportion of warrants yielding information used in the prosecution of an offence, and the average cost per warrant. This provision is in accord with Recommendation 12 of the Barrett Review.

OVERSIGHT BY INDEPENDENT BODY

Another important feature of the Act is the provision for independent oversight of the use of interception. Sections 82 and 83 of the Act give the Commonwealth Ombudsman a supervisory role over Commonwealth agencies' use of interception powers. The Ombudsman must inspect Commonwealth agencies' records to ascertain the extent of compliance by the agencies' officers with sections 79, 80 and 81, which relate to various record-keeping and destruction requirements.

The Ombudsman reports on the results of these inspections to the Attorney-General (s. 84). The Ombudsman is empowered to report on *any* breaches of the Act which are identified as a result of an inspection, not only those which relate to record-keeping requirements (s. 85). The office has extensive coercive powers under the Act to facilitate this watchdog role.[18]

On the State level, the Act requires the same functions and powers to be vested in an appropriately resourced independent authority. Victoria and New South Wales have vested the powers and functions in the State Ombudsman; in South Australia the Police Complaints Authority undertakes the function (Commonwealth Attorney-General 1993, p. 7).

At the Commonwealth level, the question of whether the oversight function should be vested in the Ombudsman or the Privacy Commissioner has been raised on a number of occasions in the last few years. The 1991 review of the Act conducted by the Commonwealth Attorney-General's Department pointed out that the Ombudsman at that time, and his predecessor, were of the view that the function would be more appropriately vested in the Privacy Commissioner. However, the review team considered that as a matter of principle the inspecting function belonged more appropriately with the Ombudsman because of the largely auditing nature of the inspections (1991, p. 64).

The matter was raised again in the Barrett Review, which recommended that the function be transferred to the Privacy Commissioner (Recommendation 6). Barrett argued that '[t]he audit function [did] not appear to sit well with the Ombudsman's office. Moreover, the accent should be on the protection of privacy rather than simply being an audit of administrative processes' (1994, p. 60). The Government again rejected this recommendation on the grounds that the present arrangements were working well and were also better suited to the Ombudsman's functional responsibilities, as 'the inspection function is one which is directed towards compliance rather than adjudication of privacy issues' (Australia, Senate 1994).

[18] For example, s. 88 of the Act provides that, notwithstanding any other law, persons are not excused from giving information or answering questions required by the Ombudsman.

CONCLUSION

This chapter has outlined the main features of the *Telecommunications (Interception) Act* and, where relevant, compared its provisions with Queensland legislation covering the use of listening devices and other forms of electronic surveillance. Some key differences are that the Commonwealth Act:

- is much more specific about the matters to be addressed in a warrant application
- specifies precisely the types of offences for which warrants may be sought
- lists a wider range of factors which have to be considered by a judge when deciding whether to issue a warrant, including whether the information could have been obtained by less intrusive means
- sets down detailed recording and reporting requirements, including a requirement that a relatively comprehensive public annual report be compiled
- requires independent oversight by an Ombudsman or some equivalent authority of record-keeping practices and the use of interception powers by agencies
- under proposed amendments will provide a civil remedy to persons whose communications have been unlawfully intercepted.

The chapter has also identified aspects of the Commonwealth scheme which are open to criticism. For instance, the period for which warrants may be issued under the Act is substantially longer than that recommended by the Commission in relation to listening devices. The Commission has also taken a different view from the Commonwealth on the issue of whether targets should be notified that they have been the subject of surveillance. However, overall, the Act is more detailed in its requirements and contains considerably more safeguards and accountability mechanisms than does State listening device legislation.

CHAPTER 4

SHOULD THE QUEENSLAND POLICE SERVICE AND THE CRIMINAL JUSTICE COMMISSION BE GIVEN TELECOMMUNICATIONS INTERCEPTION POWERS?

INTRODUCTION

This chapter addresses the question of whether the QPS and the Commission should be given the power to intercept telecommunications, subject to the requirements of the *Telecommunications (Interception) Act*. The specific issues examined are:

- the law enforcement benefits of telecommunications interception
- the adequacy of the safeguards contained in the *Telecommunications (Interception) Act*
- whether State investigative agencies need to have direct access to interception powers.

The chapter concludes with a brief discussion of some procedural and policy matters which will need to be addressed if it is decided to give the QPS and the Commission interception powers. These matters concern:

- the likely cost of establishing a telecommunications interception capability in Queensland
- which independent body should exercise the oversight role required by the Act
- the extent to which there should be consistency between State legislation governing the use of listening devices and provisions relating to telecommunications interception.

LAW ENFORCEMENT BENEFITS

Telecommunications interception is only one of a range of complementary investigative techniques. It is not always the most appropriate technique and, in any case, may only be used where the judge has considered the viability of other, less intrusive, investigative methods. However, this form of surveillance has some distinct advantages as a surveillance technique, relating particularly to:

- the importance of telephones as a means of communication
- the low likelihood of this form of surveillance being detected
- the cost effectiveness of telecommunications interception compared to other surveillance techniques
- the cogency of evidentiary material obtained through telephone intercepts.

THE ROLE OF TELEPHONES IN CRIMINAL ACTIVITY

Telecommunications interception is especially useful for investigating offences which have no identifiable victim or complainant. Such offences can be characterised as consensual crime and include offences such as official corruption and money laundering.

The telephone is an important means of communication in many criminal enterprises and acts. It is well documented that a substantial amount of the planning of many organised crimes is conducted over the telephone. For instance, the Fitzgerald Inquiry (1989, p. 195) pointed out that the telephone network is of crucial importance to the illegal SP bookmaking and gambling network. The Inquiry stated more generally that:

> . . . there is not the slightest doubt that criminals intercept telephone conversations (sometimes with the corrupt aid of officials) nor is there the slightest doubt that criminals use the telephone system for criminal purposes. (p. 173)

The reliance which many criminals place on telephones has also been recognised by Justice Stewart, who has commented that the suspect who does not wish to use a telephone is '. . . deprived of a most valuable method of communication and is forced into activities detectable by other means such as visual surveillance' (Stewart Commission 1986, pp. 341–342).

In relation to listening devices, criminals increasingly have their premises "swept" for devices or, more commonly, purposely create "house noise", such as televisions and radios left on at high volume, to ensure their conversations are not overheard. However, it has been the experience of law enforcement agencies that even when people suspect, or have been told, that their telephone is being monitored, many will continue to use it. Further, although the targets of surveillance themselves may be guarded, they will often continue to receive calls from other parties who are unaware that these calls are being intercepted (Barrett Review 1994, p. 92).

In the longer term the investigative utility of telecommunications interception powers may be diminished by the unregulated release on to the market of new communication technologies, such as digital telephony and encryption, which are more difficult to intercept. However, the Barrett Review concluded that, despite the currently decreasing network coverage and the probable rise in cost of telecommunications interception between 1994 and 1997 (see below), telecommunications interception was likely to be of considerable continuing importance in dealing with serious crime and security issues over the next three years (p. 7).[19]

REDUCED RISK OF DETECTION

Physical surveillance and the installation or removal of surveillance devices from private premises is often conducted at some risk to the personal safety of the officers involved. Moreover, if officers are detected, or there are signs of a break-in or of the disturbance of property, this is likely to alert a suspect to the possibility of a police investigation. The risk of detection is reduced, if not eliminated, by the use of telecommunications interception, as it is rarely necessary for an operative to enter private premises or property. As detailed in the previous chapter, in 1992/93 there were only three

[19] The Barrett Review found that there was insufficient information available to make projections about the telecommunications industry beyond 1997, when the industry will be fully deregulated. Barrett therefore recommended (Recommendation 1, p. 10) that a further review be carried out in that year, as it would permit a 'much better understanding of the likely telecommunications market and the requirements for, and difficulties with, interception in such an environment' (p. 5).