Telecommunications (Interception) Amendment Bill 1994

Introduction

1.1 On 6 March 1995 the Senate Selection of Bills Committee referred the *Telecommunication (Interception) Amendment Bill 1994* to the Committee for inquiry and report[1]. The Committee was required to report by 28 March 1995. Leave from the Senate was sought and the date to report was deferred to 29 March 1995.

1.2 The *Telecommunications (Interception) Amendment Bill 1994* ('the Bill') amends the *Telecommunications (Interception) Act* 1979 ('the Principal Act') and the *Telecommunications Act* 1991 ('the Telecommunications Act'). The Bill contains amendments arising out of two processes: the review conducted by Mr Pat Barrett, Deputy Secretary, Department of Finance, and the saga surrounding the Casualties of Telecom ('CoT Cases').

The Purpose of the Bill

1.3 The Main objectives of the Bill are:

- to expand the range of offences for which warrants can be obtained;
- to create a special register with the details of warrants which do not directly or indirectly lead to a prosecution;
- to create a new civil right of action against a person who unlawfully intercepts or publishes a telephone communication;
- to prohibit the disclosure of designated warrant information;

---

[1] *Journals of the Senate* No 145 6 March 1995 3025.

- to provide that more detail is required to be presented in the annual reports to Parliament;

- to tighten up the exceptions to the prohibitions on interception by a carrier employee in the course of his or her duties; and

- to amend the Telecommunications Act to make it a licence condition that holders of general and mobile carrier licences are to bear the cost of creating or developing an interception capacity on existing and new telecommunication services that may be introduced.

Background

1.4 Section 51(v) of the Commonwealth Constitution confers legislative power on the Parliament to make laws with respect to postal, telegraphic, telephonic and other like services. This placitum is the basis of the Commonwealth's power with respect to the interception of telephone calls. Telephone interception could also likely be characterised under the defence power in times of war.

1.5 Up until 1960 there was no Commonwealth legislation dealing with telecommunications interception. Phones were 'tapped' as an executive act. From 1950 onwards there were Prime Ministerial directions in place to govern the exercise of the executive discretion. These directions authorised interception only in relation to cases of espionage, sabotage and subversive activities.

1.6 The first attempt to legislatively regularise the Commonwealth's role in telephone tapping occurred with the passing of the *Telephonic Communications (Interception) Act* 1960. This Act made it a criminal offence to intercept telephonic communications, with the exception of interceptions by officers of the Post Master-General's Department for technical reasons and pursuant to warrants issued to the Australian Security Intelligence Organisation (ASIO) in connection with national security matters. There was no capacity for telephone interception for law enforcement purposes.

1.7 The 1960 Act was repealed and replaced by the

Telecommunications (Interception) Act 1979. The main innovation of this Act was that it permitted law enforcement agencies to intercept telephone calls in certain circumstances.

The Structure and Operation of the *Telecommunications (Interception) Act* 1979

1.8 The Principal Act prohibits the interception of telecommunications except where authorised in special circumstances or for the purposes of tracing the location of callers in emergencies and for related purposes.

1.9 The Principal Act creates a Commonwealth monopoly of legal telephone interception and seeks to protect the privacy of individuals who use the telecommunications system by specifying the circumstances under which it is lawful for an interception to take place. The Commonwealth's pre-eminence in the area was confirmed in the case of *Edelsten v Investigating Committee of New South Wales*[2] which held that the Act was intended to 'cover the field' and would render inoperative any State legislation which could be construed as applying to telecommunications interception.

1.10 The Principal Act criminalises telephone interception (section 7) except where permitted by the Act. Permissible intercepts are those done pursuant to a warrant issued under the Act and a broad exception [subsection 7(2)] allowing an employee of a carrier "in the course of his duties" to intercept telecommunications for or in connection with:

> "(a)(i) the installation of any line, or the installation of any equipment used or intended for use in connection with a telecommunications service or the operation or maintenance of a telecommunications system;
>
> (aa) the interception of a communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line."

1.11 This exception is considered necessary to allow proper

[2] (1986) 7 NSWLR 222.

installation, maintenance and operation of a telecommunications network and to avoid an employee becoming guilty of unlawful interception through their legitimate work activities.

1.12 The alleged misuse of this capacity to intercept is, in part, the subject of the Casualties of Telecom saga.

1.13 The Principal Act gives the power to legally 'tap' to the Australian Federal Police (AFP) and the Australian Security and Intelligence Organisation (ASIO) and creates a structure for the power to be delegated to State police services and investigatory bodies which are able to fulfil the requirements imposed by the Act. The National Crime Authority does not possess status under the Principal Act. The AFP is used by the National Crime Authority to do its telecommunications interception. The Act imposes onerous record keeping and reporting requirements on Commonwealth bodies and the Act demands that similar requirements are imposed on the State bodies through the State legislation which directly regulates the area.

1.14 State police force or investigatory body which wish to be able to access telecommunications intercept facilities need to fulfil the following criteria imposed by the Act:

1. The organisation must be designated by the Act as an 'eligible authority'. All state police forces are eligible authorities. The NSW Crime Commission, Independent Commission Against Corruption, Royal Commission into the New South Wales Police Service and Queensland Criminal Justice Commission are also eligible authorities. (Section 5)

2. The relevant state body must have complementary (State) legislation, described as the "relevant law", which complies with the requirements set out in section 35. This section provides that where state bodies exercise telephone tapping facilities in accordance with the Principal Act, record keeping and reporting procedures need to be observed on a par with those required of Commonwealth bodies exercising the same facility.

3. After the relevant law is enacted in the State the State Premier must make a request under subsection 34(1) that the

Commonwealth Attorney General "declare an eligible authority of the State to be an agency for the purpose of this Act."

1.15 The most recent additions to the list of organisations which are "eligible authorities" are the Royal Commission into the New South Wales Police Service and the Queensland Criminal Justice Commission. The Royal Commission into the New South Wales Police Service does not possess a telecommunications interception capacity as it was refused permission under subsection 34(1). The Queensland Criminal Justice Commission has recently issued a report[3] which recommends that the Commission and the Queensland Police be furnished with telecommunication interception powers. The report is presently being considered by the Queensland Parliament's Criminal Justice Committee which will be making a recommendation as to whether complementary legislation should be introduced and the Attorney's permission sought.

1.16 In 1987 the Principal Act was amended. One of the main amendments was that all warrants were required to be executed by the newly created Telecommunication Interception Division of the AFP. This includes warrants granted to States and agencies under State legislation.

1.17 The Principal Act provides a comprehensive list of the range of offences for which interception warrants may be obtained. The Principal Act defines two classes of offences for which warrants may be sought[4]. Class 1 offences include murder, kidnapping, serious narcotic offences under the *Customs Act* 1901 (Cth) and aiding, being concerned in or conspiring to commit those offences. Class 2 offences include offences against a provision of Part VIA of the Crimes Act 1914 and offences which carry a maximum period of imprisonment of at least seven years and 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;

---

[3]Criminal Justice Commission *Telecommunication Interception and Criminal Investigation in Queensland: A report* January 1995.

[4] Both are defined in section 5.

- serious fraud;
- serious loss to the revenue of the Commonwealth or a State; or
- aiding, being concerned in, or conspiring to commit any of these offences.

1.18 One of the features of the Bill is that it will extend the class 2 offences to include money laundering, corruption and organised crime. This innovation is consistent with the recommendations of the Barrett Report.

Application Procedure

1.19 All applications for interception warrants, whether from a Commonwealth or State law enforcement body, can only be made to a Federal Court judge.

1.20 Sections 41 and 42 deal with the material that needs to be included in an application. An application needs to set out the facts and other grounds on which the application is based, specify the period for which the warrant is sought and why any particular duration is considered necessary, the number of previous applications in relation to particular persons made by the organisation and the results of the previous applications and the use that the agency made of any information obtained. The maximum time for which an intercept warrant can be granted is 90 days (Section 49).

1.21 A Judge may require that further information is given on oath (section 44).

1.22 A Judge may authorise entry onto premises for the purpose of installing, maintaining, using or recovering interception equipment if he or she considers it impractical not to do otherwise (section 48).

1.23 There is a facility for urgent applications for intercept warrants (section 40(2)); the reasons for urgency need to be disclosed and the usual affidavit needs to be filed afterwards. The Judge can revoke the warrant if information filed afterwards is considered deficient (section 52). There is a facility for the AFP and State police forces to conduct intercepts without a warrant in certain circumstances [subsection 7(4) and (5)]. An application for a warrant must be made as soon a

practicable after the interception [section 7(6)].

Matters relevant to a Judge when Considering an Application.

1.24 In relation to class 1 offences section 45 states that a Judge must consider the following factors in deciding whether to issue an interception warrant:

- whether formalities of sections 41 and 42 have been complied with;
- whether there is a reasonable ground for believing that a particular person will use the service sought to be intercepted;
- whether information likely to be obtained by the interception under the warrant is likely to assist in connection with the investigation of the class 1 offence;
- whether other methods of information gathering have been utilised; and
- whether methods other than telecommunications interception would prejudice the investigation of the alleged offence.

1.25 The proceedings are ex parte, there being no opportunity for persons other than the applicant to cross examine or otherwise question the evidence tendered in support of the application.

Record-Keeping and Reporting Requirements

1.26 The Principal Act requires that Commonwealth and State agencies must retain comprehensive records of specific information concerning each warrant application (sections 80-81). The Act also requires that the AFP keep a register of all warrants issued to all agencies.

1.27 The Act further requires that the chief officer of Commonwealth agencies must provide to the Attorney General copies of all warrants issued and reports on use made of intercepted information. The Attorney must address these matters in an annual report to Parliament (section 94).

1.28 An important feature of the accountability mechanism of the Principal Act is that it envisages 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 ensure that they have complied with the various record keeping and destruction requirements. The Ombudsman has to report breaches to the Attorney General and has powers to obtain information in relation to breaches.[5]

1.29 At the State level, the Act requires that the same functions be given to an appropriately resourced independent authority. In NSW and Victoria the functions are performed by the State Ombudsman while in South Australia the Commonwealth Ombudsman undertakes the function.

The Barrett Report

1.30 The Bill seeks to implement certain recommendations of the Barrett Review of the Long Term Cost-Effectiveness of Telecommunications Interception. An unclassified version of the report was released in March 1994. Mr Pat Barrett is a Deputy Secretary in the Department of Finance. The main term of reference for the review provided that:

> The objective of the review will be to assess the future of telecommunications interception and the conditions which must be met if it is to be cost-effective in the long run (including recommendations as to the type of telecommunications interception capability Australia should maintain and the means by which it should be funded).

The Main findings of the Barrett Report

1.31 All the findings of Mr Barrett need to be appraised within the context of imminent deregulation of the telecommunications industry in 1997 and the proliferation of technologies which are neither fully regulated nor susceptible to interception in terms of the existing model of telecommunications interception. Mr Pat Barrett considers it a central issue of the review that developments in deregulation, new technologies

[5] Section 88.

and internationalisation of Australia's telecommunication network will have the effect of seriously eroding the effectiveness, long term cost effectiveness and reach of Australia's telecommunication interception capacity.[6] Recommendation No. 1 of his report was that a further review take place in 1997.

1.32 The Main findings of the Barrett review were:

- telecommunications interception (TI) is a very effective part of an integrated framework of surveillance, it being both cost effective and generally effective;

- the way in which telecommunications interception is being conducted is consistent with the requirements of the Act; and

- more privacy focussed inspections and greater transparency through notification procedures and additional reporting would further enhance privacy.

1.33 Four of the specific recommendations made by Mr Pat Barrett have been incorporated into the Bill. These recommendations are that:

1. 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);

2. a civil right of action be available to a person whose communication is unlawfully intercepted (Recommendation 8);

3. agencies' reporting obligations be extended to included the average cost of each interception and a general indication of the proportion of the warrants yielding

[6] Barrett Report p4 and p9.

information used in the prosecution of an offence (Recommendation 12); and

4. agencies' reports on the execution of particular warrants include an assessment as to how useful the information was and whether it lead to an arrest or was likely to do so (Recommendation 13).

1.34 Only two of the recommendations of the Barrett report have been explicitly not adopted. The Commonwealth has rejected the proposal that the inspection and reporting function currently carried out by the Commonwealth Ombudsman be transferred to the Privacy Commissioner (Recommendation 6). The Commonwealth has further rejected the proposal that agencies be required to notify any innocent person whose telephone service has been intercepted of the interception within a period of 90 days after the cessation of the interception (Recommendation 7). The recommendation contained an alternative proposal and this has been accepted; namely that agencies should be required to maintain a register of incidents where the telephone of an innocent person has been intercepted. This register should be made available to the relevant inspection agency for inspection and report to the Attorney General.

The Casualties of Telecom ('COT Cases')

1.35 The CoT Cases are a loose association of persons, mainly engaged in small business, who have experienced difficulties in the delivery of telecommunication services by Telecom and have complained of malpractice and illegal use of telephone interception facilities by Telecom against them. All their experiences with Telecom are essentially individual although there is some commonality in their complaints and treatment by Telecom.

1.36 The main complaints of the original CoT cases were:

1. No ring received - the caller dials a number and hears the appropriate tone but the recipient's phone does not ring;

2. The engaged tone is heard when the phone is not engaged;

3. Calls drop out;

4. The recorded message 'this number is not connected' is heard when the number is connected; or

5. Rotary numbers do not work, ie there is one number but several lines, common with businesses which advertise one number but have several lines to receive multiple calls. These facilities have apparently not worked.

1.37 The CoT cases made complaints to Telcom concerning these problems and their original complaints were allegedly met with unhelpful and glib responses. Typically Telecom found that "No fault has been found." Telecom originally denied there was a problem but unbeknown to the complainants started seeking to rectify the faults. Part of the complaint by the CoT cases was that they were told that there was no problem while Telecom was internally expending quite significant energy in addressing the issues raised. It is also alleged that Telecom was attempting to fix the problem while publicly blaming the individual complainants.

1.38 In some cases Telecom did monitor calls and has admitted as much; Ms Anne Garms is an example.[7] In other cases it still remains unclear whether interceptions have taken place.

1.39 The matter came to the attention of the Parliament in mid 1993. Both the Coalition and the Democrats championed the issue. It was decided that the appropriate course of action was an inquiry by the industry regulatory authority, Austel. Previously Telecom had engaged the firm of accountants, Coopers and Lybrand, to conduct an inquiry into their handling of customer complaints. This report was highly critical of Telecom. On 13 April 1994 Austel released a report into the CoT cases which substantially supported the criticisms that the CoT cases had made against Telecom. The Austel report found that Telecom had been hostile to customers, had taped telephone conversations and had failed to admit that there were faults in customers phones. Austel through the course of its inquiry also discovered evidence of interceptions of CoT case members and recordings of their calls.

---

[7] Report by Austel *The COT Cases* April 1994 p 206.

1.40 Both reports recommended that arbitration be pursued by Telecom with the CoT cases. These arbitration proceedings are yet to be finalised. There are presently three arbitration proceedings on foot.

1.41 Part of the problem was the lack of coherent internal guidelines for interception and one result of the process was that the Telecommunication's Ombudsman negotiated new guidelines for interceptions with Telecom. They have become the industry standard but do not have the force of law.

1.42 In December 1993 the practices of Telecom in intercepting calls became public knowledge and were referred to the appropriate law enforcement agencies by the Attorney General. This has resulted in the amendments contained in this Bill relating to section 7 and the gathering of a brief of evidence by the Commonwealth Director of Public Prosecution ('DPP') as to whether employees of Telcom should be charged for unlawful interceptions. On 8 March 1995 the DPP announced that no charges would be laid against any Telecom employees in relation to allegations of illegally intercepted telephone calls.

The Committee's Inquiry

1.43 The Committee received 20 submissions. Appendix 1 lists the names of those who made submissions. The Committee held three public hearing to discuss the provisions of the Bill in Canberra on 21, 23 and 27 March 1995 . Appendix 2 lists the persons and organisations who gave evidence to the Committee at the three public hearings.

The Bill

Part 1

1.44 This part will insert a new section 5D into the Principal Act. This clause will, if enacted, expand the category of what the Principal Act terms 'class 2 offences'. The effect of this will be to make offences that involve 'bribery or corruption' of, or by ` a Commonwealth, State or Territory official'; 'planning and organisation' (organised crime) and money laundering, the basis for an application for an interception warrant.

1.45 The term 'bribery and corruption' is not defined on the basis, according to the Explanatory Memorandum, that "the concepts are well settled."

1.46 The term money laundering is defined in terms of the statutory offences of money laundering.

1.47 The category of offences involving 'planning and organisation' is extensively defined (organised crime). The offence needs to involve a maximum penalty of at least 7 years, involve 2 or more offenders and "substantial planning and organisation" and the use of "sophisticated methods and techniques". The definition further lists at paragraph 5(3)(D) offences which must be the object of the planning. This amendment potentially gives very wide powers to eligible authorities to intercept telecommunications although the precise width will depend on how Federal Court judges interpret "substantial planning and organisation" and "sophisticated methods and techniques."

1.48 Clause 3 states that these amendments apply to offences committed before or after those amendments come into force.

1.49 There was some concern over the extension of the list of warrantable offences. Ms Beverly Schurr, New South Wales Council for Civil Liberties, stated in her evidence before the Committee that:

> "..the first provision in this bill that I want to address is the expansion of the definition of class 2 offences so that even more phone taps can be applied for in Australia.
> Harking back to the old days in 1986 you will recall that the Joint Select Committee on Telecommunications Interception reported that only the most serious offences should be eligible for phone tap warrants to be issued; that the number of offences should be kept to a minimum. The Council for Civil Liberties opposes the expansion of the definition of class 2 offences to include offences involving planning and organisation as being too broad and not being within the spirit of the joint select committee's recommendation back in 1986."[8]

[8]Evidence L&C (21 March 1995) 442.

1.50 Mr Phillip Bradley of the New South Wales Crimes Commission supported the expansion of the category of warrantable offences although with some qualification. Mr Bradely stated in his evidence to the Committee that:

> "As to the categories of offences, it is obviously necessary that the range of offences be extended and we have been saying so for a very long time indeed. There are a couple of specific things there which need to be attended to. Most of these things I have dealt with by way of correspondence with the Attorney-General's Department and Mr Barrett during the course of the review. I do not know whether it has been fixed yet, but I understood at one stage the bribery and corruption offence which had been brought within the ambit of the class 2 offences did not touch politicians. If that is still the case, I think it is an unfortunate oversight. I am thinking of cases where someone might attempt to bribe a politician, even an unwitting politician. Not being able to deal with that sort of situation is, I think, a significant limitation of the present scheme.
>
> **CHAIR**–Was that raised? I cannot remember the issue that Mr Bradley is raising now.
>
> **Ms Atkins**[9]–The bribery and corruption offence picks up bribery and corruption of an officer of the Commonwealth, state or territory, so, no, it would not pick up politicians.
>
> **Mr Bradley**–We remember the Rex Jackson case in NSW, for example, where some people were trying to influence decisions made about persons in prisons by supplying a minister with tickets and the minister went to jail for that. I think that is an oversight that ought to be dealt with. Also offences such as the perversion of the course of justice. We get cases not uncommonly where people try to influence juries and suborn witnesses, and they do not do it by fronting them in the precincts of the court and offering them money or threatening

[9] Principal Government Lawyer, National Security Branch, Attorney General's Department.

> them, they do it by telephone and letter and more subtle methods. And where the telephone is used, it ought to be possible to intercept, because these are very serious offences which attack the fabric of our democratic system, in my view. It is good to see that at last bribery and corruption is being addressed but, to the extent to which they have missed a couple." [10]

1.51 The Committee notes that it is, perhaps, inevitable in a regime that seeks to specify the type of offences in which telecommunications interception can be used that a perception might arise that there are gaps in coverage. The Committee nevertheless believes that the new offences to which the Bill seeks to extend telecommunications interception capability are of such a serious nature as to warrant the use of interception. In particular the Committee strongly endorses the recommendation of Mr Pat Barrett that interception warrants should be available for the investigation of organised crime.[11]

Part 2

1.52 This section deals with the creation of a special register of warrants. The Principal Act presently requires only a 'register' of warrants issued (section 81A) and the maintenance of records detailing each application made, whether successful or not (section 81). If Part 2 is enacted there will be a 'register' and a 'special register'. The 'special register' will identify any interception warrants which do not lead, directly or indirectly, to prosecutions. The proposed subsection 81C(1) imposes on the Commissioner of the AFP an obligation to have a special register of warrants kept and proposed subsection 81C(2) specifies that the material kept in the register needs to be the same as the information required under the existing register.

1.53 The proposed subsection 81C(3) deals with the criterion of what will be a 'registrable expired warrant.' The warrant can be renewed,

---

[10] Evidence L&C (21 March 1995) at 420. Similar concerns relating to the failure to cover politicians under bribery and corruption provisions was expressed by Mr Kevin O'Connor, Privacy Commissioner, Human Rights and Equal Opportunity Tribunal, at 446.

[11] Barrett report p10

but if three months after it has been allowed to lapse "no criminal proceeding had been instituted, or were likely to be instituted" the warrant then is registrable as a special warrant.

1.54 This proposed section is the 'fallback' provision contemplated by Pat Barrett. His primary recommendation was that "agencies should be required to notify any innocent persons whose telephone has been intercepted of the fact of interception 90 days after the cessation of the interception."[12] The justification for the complete transparency is privacy and the fact that a requirement of individual notification will function as a motivation for prudent use of the power to intercept. The Commonwealth Privacy Commissioner was a strong supporter of this recommendation in the review conducted by Pat Barrett.[13]

1.55 The establishment of the special register was supported by Mr Kevin O'Connor, Privacy Commissioner, Human Rights and Equal Opportunity Commission, in his evidence before the Committee:

> "In a democratic society, there is some point at which individuals should be informed of the visitation of secret surveillance upon them, and I would not like to see that issue lost from the agenda. But, on the other hand, I acknowledge that, whilst not accepting that proposal, this special register is an attempt to plug the gap by introducing the Minister into the question of warrants that prove not to be effective–in the sense of not leading to a prosecution–and by giving him an opportunity to oversee the matter."[14]

1.56 The Committee concurs with the sentiment expressed by Mr O'Connor and believes that the establishment of a special register is a desirable innovation in terms of the protection of individual privacy.

---

[12]Report 16.

[13] Ibid p62.

[14]Evidence L&C 21 March 1995 447