

THE PARLIAMENT OF THE COMMONWEALTH OF  
AUSTRALIA

*Telecommunications (Interception)  
Amendment Bill  
1994*

Report by the  
Senate Legal and Constitutional  
Legislation Committee

March 1995

© Commonwealth of Australia 1995

This document was produced from camera-ready copy prepared by the Senate Legal and Constitutional Legislation Committee Secretariat, and printed by the Senate Printing Unit, Parliament House, Canberra.

## **Membership of the Committee**

Senator B Cooney (Chair)  
Senator S Spindler (Deputy Chair)  
Senator C Ellison  
Senator C Evans  
Senator J McKiernan  
Senator W O'Chee

### Participating members:

Senator Abetz	Senator M Baume
Senator R Boswell	Senator D Brownhill
Senator C Chamarette	Senator B Harradine
Senator R Kemp	Senator J McGauran
Senator D Margetts	Senator J Short
Senator G Tambling	Senator A Vanstone
Senator S Knowles	

## **Committee Secretariat**

Secretary:	Ms Anne Twomey
Committee Secretariat:	Mr Stephen Bull
	Mr Peter Thomson
	Ms Marina Ellis
	Mr Don Wilkinson
Executive Assistants:	Ms Cath Drinkwater
	Ms Lois Carroll

The Senate  
Parliament House  
CANBERRA ACT 2600  
Telephone: (06) 277 3560

## Telecommunications (Interception) Amendment Bill 1994

### Contents

	Page
• Membership of the Committee	i
• Table of Contents	ii
• Introduction	1
• Purpose of the Bill	1
• Background	2
• The Structure and Operation of the Principal Act	3
• Application Procedure	6
• Matters relevant in considering an Application	7
• Record keeping and reporting requirements	7
• The Barrett Report	8
• The main findings	8
• The Casualties of Telecom	10
• The Committee's Inquiry	12
• Part 1	12
• Part 2	15
• Part 3	17
• Part 4	19
• Part 5	20
• Part 6	22
• Schedule 2	29
• Conclusion	33
• Recommendation	33

### Dissenting Report

Report of Senator Sid Spindler

### Appendices

Appendix 1	Submissions Received	34
Appendix 2	Details of Meetings	37
Appendix 3	Guidelines on Voice Monitoring or Recording of Telephone Services	45

---

# 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<sup>1</sup>. 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;

---

<sup>1</sup> *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*<sup>2</sup> 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

---

<sup>2</sup> (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<sup>3</sup> 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<sup>4</sup>. 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;

---

<sup>3</sup>Criminal Justice Commission *Telecommunication Interception and Criminal Investigation in Queensland: A report* January 1995.

<sup>4</sup> 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.<sup>5</sup>

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

---

<sup>5</sup> 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.<sup>6</sup> 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 include the average cost of each interception and a general indication of the proportion of the warrants yielding

---

<sup>6</sup> 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 Telecom 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.<sup>7</sup> 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.

---

<sup>7</sup> 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 Telecom 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 hearings 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."<sup>8</sup>

---

<sup>8</sup>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**<sup>9</sup>—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

---

<sup>9</sup> 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." <sup>10</sup>

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.<sup>11</sup>

## 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,

---

<sup>10</sup> 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.

<sup>11</sup> 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."<sup>12</sup> 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.<sup>13</sup>

**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."<sup>14</sup>

**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.

---

<sup>12</sup>Report 16.

<sup>13</sup> Ibid p62.

<sup>14</sup>Evidence L&C 21 March 1995 447

---

## Part 3

1.57 This Part creates a new regime of civil remedies for unlawfully intercepted material in addition to criminal penalties in the Principal Act and under any other Commonwealth or State law. Mr Pat Barrett made a recommendation to the effect that "a right of action against a person who unlawfully intercepts or publishes a telephone communication should be conferred on the person whose communication is unlawfully intercepted."<sup>15</sup>

1.58 The civil remedies which the Part proposes require an 'aggrieved person' to be a party to a communication or have the communication made on their behalf. The defendant needs to intercept the communication or be complicit in an interception. The civil remedy proposed by the Bill is very wide and empowers the Court to make any such orders against the defendant as the Court considers appropriate.

1.59 The proposed subsection 107A(7) "without limiting the orders that may be made under this section" lists some of the kinds of orders that a court might make. These are:

- (a) declarations that the interception was unlawful;
- (b) an order for damages;
- (c) an order in the nature of an injunction;
- (d) an order by way of restitution or as the Bill states an order that the defendant pay to the aggrieved person an amount which represents "in the opinion of the court, the total gross income derived by the defendant as a result of the interception or communication, as the case requires."

1.60 The proposed subsection 107A(8) explicitly states that the court in assessing damages may award punitive damages.

1.61 It is contemplated that this jurisdiction will be exercised by the Federal Court of Australia or "a court of a State or Territory." The proposed subsection 107A(5) further contemplates ancillary civil relief for a victim in criminal proceedings. The proposed subsection seeks to allow an aggrieved person to use the criminal proceedings under section 7 of

---

<sup>15</sup> Ibid at p16.

the Principal Act as a means to base civil proceedings against the defendant. The explanatory memorandum states:

"As the same conduct may found civil liability as well as the criminal liability, this provision saves an aggrieved person from having to present the same evidence again in a civil court."

The section appears to contemplate that civil proceedings will be 'tacked on' to the criminal proceedings, the same court handling both.

1.62 These civil remedies will bind the crown.<sup>16</sup>

1.63 The Committee did not receive any adverse evidence concerning the proposed civil remedy although Mr Kevin O'Connor did raise an important issue concerning how an individual might become aware of a possible cause of action.

"On the question of the civil remedy, it is an important advance, and I have indicated that. The Barrett report favoured a view that I have certainly put forward on other occasions that, if a warrant does not lead to criminal prosecution, the existence of that interception ought— I believe—to be notified at some point to the subjects of the interception and the warrant. The Barrett report is striking on this matter, at pages 71 and 72 of the public document, where it considers the police objections, the culture of secrecy which understandably surrounds police operations in respect of criminal investigations, and their concerns about dealing with people in this way.

Two major policing nations with whom we often compare ourselves—Canada and the US—do this. As I read the Barrett report, they are untroubled by the proposition that, at some point in the process of secret surveillance, people should be made aware of what has occurred. That is really the best antidote to improper activity, and is really made manifest tonight by these protestations from people about the

---

<sup>16</sup> Section 4.

maintenance monitoring that they feel was unfairly undertaken. They became aware of it, and they have acted to defend their rights..... it seems to me that the civil remedy will only be a measure of protection for those who somehow find out that this kind of interception has gone on. So you have this strange situation where the person against whom the warrant information is used in a trial will find out that the person who is not brought to trial will not find out. It could be argued that the person who is possibly more culpable gets an opportunity to use a civil remedy while the person who is less culpable does not. I think that is a dilemma that will need to be addressed."<sup>17</sup>

## Part 4

**1.64** This part of the Bill prohibits the disclosure of information about applications for warrants, their existence and details concerning a warrant. The proposed section 6EA defines 'designated warrant information' as:

"(a) information about any of the following:

- (i) an application for a warrant;
- (ii) the issue of a warrant;
- (iii) the existence or non-existence of a warrant;
- (iv) the expiry of a warrant; or

(b) any other information that is likely to enable the identification of:

- (i) the telecommunications service to which the warrant relates; or
- (ii) a person specified in a warrant as a person using or likely to use the telecommunications service to which the warrant relates."

**1.65** The Bill will criminalise the disclosure of 'designated warrant information' by amending section 63. In accordance with section 105, which criminalises breaches of the Principal Act generally, disclosing warrant information will carry a penalty of \$5000 or 2 years in gaol.

---

<sup>17</sup> Evidence L&C (21 March 1995) 447.

**1.66** The proposed section 63AA creates some exceptions to the prohibitions. These primarily relate to the application process, issue of warrants, record keeping and reporting requirements of the Principal Act. In each of these cases there is a practical necessity for warrant information to be disclosed.

**1.67** This provision comes from one of Mr Pat Barrett's recommendations (No.9) and faithfully follows its intent which was that the Principal Act "should be amended to prohibit the disclosure of the existence of a warrant other than in accordance with that Act."<sup>18</sup> The ostensible justification for this recommendation was that there was uncertainty as to whether the *Freedom of Information Act* applies to Telecom and specifically to warrant information. The prohibition was considered necessary to secure the privacy of individuals subject to telephone interception.<sup>19</sup>

**1.68** The Committee heard no strongly adverse evidence concerning this provision of the Bill. The Committee believes that provision will greater enhance the protection of individual privacy afforded by the Principal Act and is therefore a desirable measure.

## Part 5

**1.69** This part expands the existing reporting obligations<sup>20</sup> in response to Recommendation No. 13 of the Barrett report which stated that:

"In their reports on the execution of particular warrants, agencies should be required to include an assessment of how useful the information was and whether it led to an arrest or is likely to do so."<sup>21</sup>

---

<sup>18</sup> Barrett Report p16.

<sup>19</sup>Ibid p.64.

<sup>20</sup> Section 94 requires that the chief officer of Commonwealth agencies using intercept facilities report to the Attorney General after each warrant is issued and "as soon as practicable after" revocation as to the use made of information obtained and to whom it is communicated. Section 96 requires eligible state authorities to report yearly.

<sup>21</sup> Recommendation 13 Barrett report at p.18.



1.70 The new reporting obligations will require that information detailing the number of arrests made or likely to be made on the basis of the warrant information and an assessment of the usefulness of the information be included [proposed subsection 94(2)]. Part 5 also contains two formulae: one for giving some indication of the efficacy of interception [proposed subsection 102(3)]; and another for some measure of its cost effectiveness [proposed subsection 103(aa)]. In both cases the information needs to be communicated to the Attorney with other reporting information.

1.71 The submission of the Law Society of New South Wales criticises this section on the ground that it should contain more detail. Mr Maurie Stack, President of the NSW Law Society, noted that the reports would not assess the social and economic effects of the intercept.<sup>22</sup> The Law Society includes in its submission an alternative reporting format, modelled on American and Canadian practice, which includes notification of persons who have had their phones intercepted.<sup>23</sup>

1.72 The provision nevertheless was strongly supported by Ms Beverly Schurr, New South Wales Council for Civil Liberties, in her evidence before the Committee:

"We welcome the proposal to require, for the first time, some sort of costing information to be provided. In the past, the government has been embarrassed about the inability to provide definite financial costs for phone tapping."<sup>24</sup>

1.73 The Committee believes that these provisions are a desirable expansion in the mandatory information required to be communicated to the Minister and will, if enacted, provide a useful measure of the efficacy of telecommunications interception.

---

<sup>22</sup>Submission 8 at p2.

<sup>23</sup> Barrett Report at p18.

<sup>24</sup> Evidence L&C (212 March 1995) 442.

## Part 6

**1.74** This part deals with interception by carriers and is in direct response to the concerns raised by the CoT cases and the inquiry conducted into their complaints by Austel.

**1.75** The proposed paragraph 7(2)(a) seeks to tighten up the existing exemptions which allow employees of a carrier to lawfully intercept a communication by adding the element of necessity. The structure of the existing exemption is preserved, although the carrier will, under the proposed amendments, need to show that interception is "reasonable necessary" to do an act or thing in order to perform those duties effectively.

**1.76** A new paragraph 7(2)(aa) will place a similar limitation on the authority of independent contractors to intercept telecommunications lawfully.

**1.77** The proposed subsection 7(2) of the Bill directs a court when deciding whether an interception was "reasonable necessary" to have regard "to such matters as are specified in, or ascertained in accordance with, the regulations."

**1.78** Mr David Krasnostein, General Counsel, Telecom Australia, in his submission to the inquiry<sup>25</sup> criticised these amendments on a number of grounds. His principal objections are that the Bill seeks to impose restraints on interceptions in a way which is prejudicial and unfair to Telstra and its employees by exposing them to unreasonable risks of prosecution for criminal offences. This difficulty arises due to the inserted criterion of 'reasonable necessity'.

**1.79** Telecom\Telstra in their submission proposed an amendment to the proposed subsection 7(2A). Their proposed amendment would read as follows:

"7(2A) For the purpose of paragraphs (2)(a) and (aa), in determining whether an act or thing done by a person was reasonably necessary:

---

<sup>25</sup> Sub. 10.

(a) a court is to have regard to such matters as are specified in, or ascertained in accordance with, the regulations; and

(b) any act or thing done by a person in good faith in compliance or purported compliance with matters (including guidelines or procedures) specified in, or ascertained in accordance with, the regulations, will be taken to be reasonably necessary<sup>26</sup>

1.80 The concern raised by Telcom was echoed by a number of witnesses who gave evidence before the Committee. Ms Milligan, Industrial Officer, CEPU<sup>27</sup>, stated in her evidence that:

"The union is concerned about the legislation. In fact, we are extremely alarmed by the proposed amendments to section 7(2) of the legislation. Our view of that part of the bill is that it imposes an unreasonable and exceptionally vague test to determine the individual civil liability under the new and very wide ranging civil liabilities proposed by the Act. On our understanding that is the new imposition of the Act which has a primary significance for our members who are involved in implementing the interception procedures.

The union is specifically concerned about the situation where an employee who is acting in good faith and in strict compliance with any guidelines, or regulations which flow from the Act, may still be found by a court of law to be open to civil prosecution for their actions. We are very concerned about that situation. We believe that an employee in those circumstances should be specifically protected by the Act. I refer to the test provided for in the amendment - which will be considered by a court—that the action was reasonably necessary in order to perform the person's duties effectively. That is open to a court to review. As I understand the

---

<sup>26</sup> Sub. 10 p3.

<sup>27</sup> The full name of this organisation is the Communications, Electrical, Electronic, Energy, Information, Postal, Plumbing and Allied Services Union of Australia.

amendment, the court is directed to have reference or regard to the guidelines and regulations. But strict compliance with those guidelines and regulations is not by any means a complete defence for that employee. The employee's acts can be reviewed, and determined to be not in compliance with that test by a court of law even though the employee has done everything they possibly can do to conform with every piece of information and guideline that they have been given.

In the union's view, a complete defence in those circumstances should be made available to the employee concerned: that is, the employee carrying out their ordinary duties in an authorised manner. To this end having had the advantage of examining the submission put forward by Telstra to the committee, given the obvious sensitivity our organisation would have, we would say that we support the proposal put forward by Telstra to amend the bill at that section, section 7(2). That in our view is a critical area. Even though it is patently obvious that the prime target for such civil litigation would be the corporation, nevertheless the individual employee is open for that action. That in itself, we believe, will, at the very minimum, create extraordinary disruption to routine day-to-day activities which employees are required to carry out.

Our view is that this protection must be explicitly provided for in the bill in at least the form put forward in the submission by Telstra. Without that being taken into account in that manner, we would strongly object to the bill going forward, and we believe it is severely flawed."<sup>28</sup>

**1.81** Mr Ross Ramsay, Optus, voiced concern over the proposed amendments to section 7 and also suggested that greater reliance should be placed on internal guidelines.<sup>29</sup>

**1.82** A number of the CoT cases present at the Committee's hearing on 21 March expressed concern that the present amendments did

---

<sup>28</sup> Evidence L&C (21 March 1995) 436.

<sup>29</sup> Evidence L&C (21 March 1995) 450.

---

not go far enough in tightening up the carrier exception. Mr Graham Schorer, spokesperson, CoT cases, stated in his evidence that:

"Yes, the Senate does have a role, not only to individuals but to corporations. Everyone is going to be using the telecommunications system on this information highway. It is as open as a can of worms. But this legislation is not addressing it, because it is not going to allow the evidence to be collected to bring about the charges to stop it happening. And the individual people within Telecom are not given any encouragement to come forward on their fellow people who are doing it on their own, or are wrongly accepting instructions from those above. I believe that if there is a genuine need for proper monitoring, listening or taping of a conversation or a service, because they can do both, it should not be a matter of the telecommunications people going along to the person. If they are going to get prior written consent, they should apply to the regulator, Austel, and justify to Austel why this particular identification of fault requires this treatment. I certainly do not accept that this sort of treatment of listening and taping and monitoring is part of network maintenance. That is a lot of codswallop. Ask any technical communications consultant."<sup>30</sup>

1.83 Mr Kevin O'Connor, Privacy Commissioner, in his evidence before the Committee stated that:

" On the final question of maintenance, I put forward the view in correspondence with the department that I think the proposition of obtaining consent for all recording should at least be more actively canvassed. As I understand it, what we have at the moment is that consent is to be obtained if the recording occurs in response to a complaint but consent is not necessary if it is being undertaken for maintenance purposes in accordance with the guidelines. I would argue that, if you are going to go as far as recording, it may be appropriate that consent be obtained or possibly you can put a quantitative limit on it—for example, recording of a certain duration or of

---

<sup>30</sup> Evidence L&C (21 March 1995) 435.

a certain extent should be subject to consent.

I think there are difficulties with going that far in respect of this incidental listening and that kind of thing. I accept from what I have been told over the years by Telecom that it is inevitable in the maintenance environment that some form of listening into the lines to assess the quality of communications is necessary. I am interested in this shift from mere listening, with the risks that has in terms of redisclosure of information, and actual recording."<sup>31</sup>

**1.84** The Committee received a submission from Mr Warwick Smith, Telecommunications Industry Ombudsman, which contained a copy of Telecom's internal '*Guidelines on Voice Monitoring or Recording of Telephone Services*'. These guidelines were drafted in response to the CoT cases saga and have been adopted by Optus and Vodaphone. They appear to be establishing themselves as the industry standard. These guidelines, for example, provide that where extended voice monitoring takes place it should only occur with the consent of the customer. A copy of these guidelines is annexed to this report at appendix 3.

**1.85** In his brief submission Mr Smith supported the 'reasonableness' test but suggested that it should be strengthened by linking it with an appropriate industry code such as Telecom's internal guidelines.<sup>32</sup>

**1.86** The Committee was fortunate in its inquiry to have the assistance of Mr Michael Rozenes QC, Commonwealth Director of Public Prosecutions. The Committee heard whether the recent decision by the DPP not to charge a Telecom employee was due to a technical deficiency of the Principal Act and whether the amendments in the Bill would assist in curing any such deficiency:

" **Senator ABETZ**—As I understand it, the question that we basically wanted to ask was on the concern expressed at the last hearing that the employees of Telecom allegedly could not be charged. That is, I think, what we were advised by Mr

---

<sup>31</sup> Evidence L&C (21 March 1995) 447.

<sup>32</sup> Sub.7 p3.

Reaburn. We as a committee want to know, firstly, whether that was the case; and, secondly, whether this new bill will overcome what some people see as a deficiency.

**Mr Rozenes**—There was no prohibition on them being charged, there was just no likelihood of us recommending that course, because there was no satisfaction on my part that there were reasonable prospects of securing a conviction on the evidence then available. Were there to be admissible evidence that could have resulted in a conviction, there would have been no reason why Telecom employees could not be charged under the existing legislation.

**Senator ABETZ**—So it was only an evidentiary problem, as you saw it, as opposed to a technical problem with the legislation.

**Mr Rozenes**—Yes. There is nothing wrong with the legislation, in that it goes just so far but no further. But in attempting to obtain a conviction on the sort of evidence that one expects to get in such cases, there is no high chance of success.

**Senator ABETZ**—So getting a successful prosecution in any case would be difficult, given the framing of the legislation?

**Mr Rozenes**—I would say it would be difficult in this sort of case; and I do not see that it would be any easier under your proposed legislation, either.<sup>33</sup>

1.87 There was also discussion of a letter, dated 2 March 1995, from Mr Rozenes, tabled by Mr Robert Bray, concerning the DPP's decision not to prosecute a Telecom employee in Ballarat. In evidence before the Committee the following exchange occurred:

" **Senator SPINDLER**—I have got a question that relates to a letter that the committee received and that has been tabled. In the letter you state, Mr Rozenes, that you are not proceeding with prosecutions because as a result of legislative

---

<sup>33</sup> Evidence L&C (27 March 1995) 495.

changes made in 1991, and I quote: *Telecom employees are no longer officers of the Commonwealth for the purpose of the Crimes Act 1914.*

**Mr Rozenes**—That decision is the subject of a further review by my office at the very moment that we speak.

**Senator SPINDLER**—I see. I was just wondering whether you thought that it might be necessary, seeing that we are talking of an area that is of considerable importance in the community, that we should either seek amendments to the Crimes Act or somehow have an amendment in the telecommunications legislation to cater for this situation.

**Mr Rozenes**— I think there may be some legislation that is currently available that my office overlooked in the course of determining this matter in the first place; and as I say, that is the subject of further consideration.<sup>34</sup>

**1.88** The Committee believes that the amendments contained in this part are an improvement on the present situation. The Committee nevertheless believes that they cannot stand alone and need to be supported by appropriate regulations. The proposed subsection 7(2A), in part, provides such a vehicle. The proposed subsection reads:

"(2A) For the purpose of paragraph (2)(a) and (aa), in determining whether an act or thing done by a person was reasonably necessary in order for the person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in, or ascertainable in accordance with, the regulations."

**1.89** Telecom's internal '*Guidelines on Voice Monitoring or Recording of Telephone Services*' appear to the Committee to provide a potentially ready made model for regulations. The Committee believes that in view of the fact that an industry standard appears to have emerged, consideration should be given to making Telecom's internal guidelines, at least, the starting point for regulations. While the linkage

---

<sup>34</sup> Evidence L&C (27 March 1995) 497.



---

would not be as strong as that proposed by the Telstra amendment the Committee nevertheless believes that the giving of legal stature to the guidelines would allay the fears of both the union and industry groups concerning lack of clarity in what would be 'reasonably necessary' whilst increasing the protection afforded to individual privacy.

## Schedule 2

**1.90** This schedule amends the *Telecommunications Act*. The primary effect of these amendments is to make it a licence condition that Telecommunication carriers pay for the development of an 'interception capacity' (for law enforcement and intelligence related intercepts) on their lines. The amendments also provide that the carrier will be able to seek to recover those costs, over time, from the other party or parties [proposes subsection 72A(6)]. Nevertheless in the initial creation of an interception capability this will be borne by the carrier [proposed subsection 73A(5)].

**1.91** This implements recommendations Nos 14 and 16 of the Barrett report.<sup>35</sup> Mr Pat Barrett explicitly recommended that carriers have the capacity to recover the costs of maintaining interception capabilities from users. His rationale for such an arrangement was that:

"In keeping with the commercial orientation of the arrangements, each agency (Commonwealth or State) would contract with the relevant carrier on the basis of its individual access to the capabilities. There would be a discipline on all agencies to indicate an interest or otherwise quickly so that they could make their own cost effectiveness. There would clearly be an incentive to maximise participation to minimise cost. Moreover, it would be a real test of the collective view of the value and priority of the capability."<sup>36</sup>

**1.92** Mr Pat Barrett, in his review, canvassed an option that

---

<sup>35</sup> at p 20.

<sup>36</sup>Barrett Report p105.

carriers only be able to recover the capital costs, but not interest, associated with the establishment of telecommunications interception facilities from agencies.<sup>37</sup> The proposed regime in schedule 2 contemplates that carriers are able to recover "the costs (whether of a capital nature or otherwise) relating to the creation or development of the interception capability." This appears broader than mere capital costs, although seems to fall short of allowing a carrier to recover all the running costs associated with maintaining an interception facility.

**1.93** The Bill does not differentiate between State and Commonwealth agencies, although during the Committee's inquiry it was the State agencies who voiced concern over the introduction of an element of 'user pays'. Mr Mick Williams, Detective Chief Inspector, Victorian Police stated in his evidence before the Committee that:

"From a funding perspective, the Victoria Police are strongly opposed to the proposed amendment requiring carriers to fund interception capabilities and then recover the costs from the agencies. In our original submission we asserted that the development of interception services should be funded by carriers, and that they should in fact be recovered from subscribers. We still strongly maintain that view. There may be some who assert that under such a concept of carrier pays and recovers from subscribers, law enforcement agencies may well say that we want everything made interceptible. That is not so. In fact, a precedent has already been set under the revamped Austel new technology subcommittee, where the agencies have opted to accept interception measures that are of a lesser standard. We refer to them as interim interception measures. There have been some instances where we have said that we do not need services that are about to be released to be interceptible. We are saying that the situation will not occur where we will ask for everything to be interceptible. Some may say there will be a greater use of telephone interception. We very, very strongly reject that. As I have already alluded to, the existing stringent legislation prevents us from going on any fishing expedition or anything

---

<sup>37</sup> Ibid p 103.

like that. The legislation does not allow us to misuse it, so we reject that assertion."<sup>38</sup>

**1.94** Mr Phillip Bradley, New South Wales Crime Commission, also voiced similar concerns in relation to the funding implications of the Bill.<sup>39</sup>

**1.95** Mr Ross Ramsay, Manager, Government Liaison, Optus, expressed concern in his evidence before the committee over a suggestion that carriers should be made to pay the cost of the development and maintenance of telecommunications interception capabilities:

"I would like now to turn to another matter, raised by Mr Bradley's intervention earlier on funding. What I think Mr Bradley said was that the funding ought to be by the carriers for capital matters— I assumed it was capital matters— and that this should just find its way into customer prices. I would like to comment that there is a need for discipline on both sides of the house where funding is concerned. There are many levels of interception capability, not just one. It is not one simple matter. Some levels of interception capabilities are more costly than others, so agencies need to decide what level of interception capability is appropriate for the task, and know the cost involved and be prepared to participate in the funding."<sup>40</sup>

**1.96** After this evidence was heard on 21 March 1995 the Committee received a submission from Mr Pat Barrett, Deputy Secretary, Department of Finance. In his submission Mr Barrett stated that:

"In relation to state funding, while Ross Ramsay (Optus) raised the important question as to who should pay, the issue of charging also involves pragmatic questions about the nature and timing of significant expenditure on TI, such as for GSM and the move to digital technology on the network.

---

<sup>38</sup>Evidence L&C (21 March 1995) 418.

<sup>39</sup> Evidence L&C (21 March 1995) 421.

<sup>40</sup> Evidence L&C (21 March 1995) 450.

Having to fund such decisions, really requires an assessment by the various Agencies as to the benefits likely to be derived in the current environment and in relation to other priorities.

To the extent that Federal Agencies such as ASIO require interception capability sooner than State Agencies, the former bear the brunt of the initial expenditure. The State Agencies only pay when they use the capabilities. As well given the cost, the coordination mechanism provided by LEAC ('the Law Enforcement Advisory Committee') requires a disciplined assessment of the capability required and more particularly when it is required."<sup>41</sup>

**1.97** The Committee believes that the cost discipline which the proposed amendments will produce is desirable. This is especially the case with the proliferation of new technologies where the introduction of a cost element will force agencies to prioritise their interception needs so as to avoid an excessive burden being placed on the carriers and ultimately the subscribers to any system.

---

<sup>41</sup> Sub 19 at p1.

## Conclusions

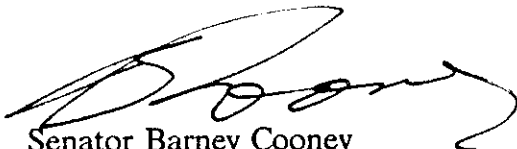
1.98 Mr Kevin O'Connor stated in his evidence before the Committee that:

"The bill is, I think, a careful attempt to bring an increased level of discipline into various aspects of the process that surrounds the obtaining of telecommunications interception warrants and, obviously, I welcome the elements of the bill that seek to incorporate greater scrutiny into the process of the effectiveness of warrants, in particular, and the cost of warrants. The reference in the bill to a civil remedy is not unimportant and is a significant new acknowledgment of the importance of the parliament protecting individual privacy interests through more accessible mechanisms than had previously existed."<sup>42</sup>

The Committee agrees with these sentiments and is satisfied that the measures contained in the Bill are necessary and should be enacted into law.

## Recommendations

**Recommendation:** A majority of the Committee recommends that the Bill as introduced be enacted.



Senator Barney Cooney  
Chair

<sup>42</sup> Evidence L&C (21 March 1995) 445.

# ***Telecommunications (Interception) Amendment Bill 1995***

## **Dissenting Report**

**Senator Sid Spindler**  
(Australian Democrats, Vic.)

---

The evidence before the Committee indicated a high level of concern about the monitoring and recording of phone conversations without customer consent. On the other hand, random and brief monitoring is regarded as essential for the operation and maintenance of telephone systems, and a requirement to obtain consent in such cases would appear to impose an unreasonable burden on carriers.

The evidence indicates that the non-random covert monitoring of customers' phone services has happened in some cases in sensitive circumstances. It also shows such interception can traumatise the target customer.

In particular, the provisions of the Bill attracted the following criticisms:

- Telecom, Optus and the CEPU voiced concerns that carriers and their employees would be exposed to unreasonable legal risk. Telecom claimed that acts done in good faith for maintenance or operational purposes, in accordance with guidelines referred to in the regulations, could nevertheless be found by a court not to be reasonably necessary.

The uncertainties created by the legislation were made worse by the fact that the regulations have not been made public, making it difficult to assess the impact of the legislation.

- The Casualties of Telecom called for the involvement of AUSTEL in giving approval for voice monitoring and recording, to bring independent expertise to bear in deciding whether such monitoring and recording was necessary.
- The Privacy Commissioner called for examination of a requirement of customer consent for all voice recording.

The inability of the Director of Public Prosecutions to take action under the *Crimes Act* in relation to the apparently unwarranted disclosure by a Telecom employee of a customer's private information, due to amendments of the *Crimes Act* passed in 1991, was the subject of related evidence.


### ***Recommendations***

- The Bill should not be proceeded with until the proposed regulations are available.
- The Bill should be amended to:

- » require written customer consent to the recording or protracted voice monitoring of conversations on that customer's telephone service. This should not include random and brief interceptions as described in the Telecom submission. Failure to obtain written consent should be made an offence.
  - » provide carrier employees with a defence of good faith.
- Sanctions, similar to those previously available under the *Crimes Act*, should be available to deal with the unwarranted and unauthorised release of private information held by a carrier.

**Comment**

Given the strong opposition of most witnesses to the provisions dealing with interception by a carrier for operational or maintenance purposes, it seems extraordinary that the majority report presses for the passage of the Bill as drafted.

  
Senator Sid Spindler  
(AD, Vic)

**Appendix 1**  
**Submissions Received**



## APPENDIX 1

### *Telecommunications (Interception) Amendment Bill 1994*

#### List of Submissions

Sub No.	Individual/Organisation	Date of Submission
1	Human Rights and Equal Opportunity Commission, Ms Lindy Smith	23.02.95
2	Attorney-General's Department, Ms Liz Atkins	24.02.95
3	Criminal Justice Commission, Mr R S O'Regan QC	24.02.95
4	Australian Telecommunications Authority, Mr Neil Tuckwell, Chairman	24.02.95
5	South Australia Police, Detective Senior Sergeant D R Kossatz	24.02.95
6	Department of Finance, Mr O Winder	27.02.95
7	Telecommunications Industry Ombudsman, Mr Warwick Smith	27.02.95
8	The Law Society of NSW, Mr Maurie Stack	02.03.95
9	Northern Territory Police, Mr Brian Bates	06.03.95
10	Telecom Australia, Mr David Krasnostein	07.03.95
11	Minister for Police and Emergency Services, Dr Frank Madill	13.02.95
12	Commonwealth & Defence Force Ombudsman, Mr David Parkinson	16.03.95
13	<b>NOT RELEASED</b>	
14	South Australian Police, Detective Senior Sergeant D R Kossatz - Supplementary Submission	21.03.95
15	Independent Commission Against Corruption, The Hon B S J O'Keefe, AM QC	21.03.95

16	South Australia Police, Detective Superintendent Barry England	21.03.95
17	Communications, Electrical, Electronic, Energy, Information, Postal, Plumbing and Allied Services Union of Australia, Ms Julie Milligan/Mr John Saunderson	21.03.95
18	Attorney General's Department - Supplementary Submission, Ms Liz Atkins	21.03.95
19	Department of Finance, Mr P J Barrett	22.03.95
20	Privacy Committee - NSW, Ms Maureen Tangney	27.03.95

## Appendix 2

### Details of Meetings

## APPENDIX 2

### Details of Meetings

**Public Hearing:** 21 March 1995  
7.45 pm  
Adjourn: 11.45 pm  
Committee Room 2S1  
Parliament House  
CANBERRA

**Attendance:** **Committee Members**

Senator B Cooney (Chair)  
Senator S Spindler  
Senator C Ellison  
Senator J McKiernan

**Participating Members**

Senator Abetz  
Senator Boswell

**Witnesses:**

**Attorney General's Department**

Mr Norman Reaburn

Deputy Secretary

Ms Liz Atkins

Principal Government Lawyer

Mr Chris Gallagher

Senior Government Lawyer

**Department Communications and the Arts**

Ms Fay Holthuyzen

First Assistant Secretary

Telecommunications Industry Division

Mr Tom Dale

Acting Assistant Secretary

Regulatory Policy Branch

**Department of Finance**

Mr Pat Barrett

Deputy Secretary

**Australian Federal Police**

Mr Alan Mills

Assistant Commissioner

Mr Geoffery Penrose

Detective Superintendent

**Telecom/Telstra**

Mr Michael Pickering

Group Manager - Corporate Policy

Ms Joy Geary

Special Counsel, Litigation

Mr John Seamons

National Manager - Network Performance

**CEPU**

Mr John Saunderson National Industrial  
Officer

Ms Julie Milligan National Industrial Officer

**Optus**

Mr Ross Ramsay

Manager Government Liason

**Commonwealth Ombudsman**

Ms Sue Pidgeon

Senior Assistant Ombudsman

Dr D. Parkinson

Director Intercept Audit Section

**The Casualties of Telecom**

Mr Graham Schorer

Mrs Ann Garms

Mr Alan Smith

Mr Robert Bray

**National Crime Authority**

Mr Tom Sherman

Chairman

**NSW Crime Commission**

Mr Phillip Bradley

Chairperson

**Victorian Police Department**

Paul Hornbuckle

Superintendent

Mr Mick Williams

Chief Inspector

**Austel**

Ms Frances Wood

**New South Wales Council for Civil Liberties**

Ms Beverly Schurr

**Human Rights and Equal Opportunity  
Commission**

Mr Kevin O'Connor - Privacy Commissioner

**Australian Federal Police**

Commissioner Alan Mills

Assistant Commissioner

**Private Meeting:**

23 March 1995

8.40 am

Adjourn: 9.05am

Committee Room 1S5

Parliament House

CANBERRA

**Attendance:**                      **Committee Members**

Senator B Cooney (Chair)

Senator S Spindler

Senator J McKiernan

Senator W O'Chee

**Participating Members**

Senator Abetz

**Public Meeting:**                23 March 1995  
   Committee Room 1S4  
   5.07pm  
   Adjourned 5.30pm

**Attendance:**                      **Committee Members**

Senator B Cooney (Chair)

Senator S Spindler

Senator C Ellison

Senator J McKiernan

Senator C Evans

**Participating Members**

Senator Abetz



**Witnesses:**                    **Attorney General's Department**  
Mr Norman Raeburn  
Deputy Secretary

**Advisor - Minister for Justice**  
Mr Simon Overland

**Public Hearing:**                27 March 1995  
Committee Room 2S1  
7.10pm  
adjourned 7.20pm

**Attendance:**                    **Committee Members**  
  
Senator B Cooney (Chair)  
Senator S Spindler  
Senator C Ellison  
Senator J McKiernan

**Participating Members**  
Senator Abetz

**Witnesses:**                    **Commonwealth Director of Public Prosecutions**  
**Mr Michael Rozenes QC**

**Private Meeting:** 28 March 1995  
Committee Room 1S6  
6.30pm  
adjourned: 7.05pm

**Attendance:** **Committee Members**  
  
Senator B Cooney (Chair)  
Senator C Ellison

**GUIDELINES ON VOICE MONITORING  
OR RECORDING OF TELEPHONE  
SERVICES**

Released April 29, 1994

## GUIDELINES ON VOICE MONITORING OR RECORDING OF TELEPHONE SERVICES

### 1. Introduction

These guidelines detail the procedures followed by staff whenever voice monitoring or recording is undertaken on a telephone service or a telecommunications system. The guidelines set out Corporate Policy, legislative obligations and the decision making process for service quality and network maintenance and complaints handling purposes.

### 2. Coverage

In these guidelines:

- reference to voice monitoring involves listening to a voice communication passing over a telecommunications system or line;
- reference to voice recording involves recording on tape of a voice communication passing over a telecommunications system or line.

The guidelines do not deal with the use of call charge analysis equipment (CCA/E) and CLI facilities for monitoring service usage which is currently dealt with in Company policies on unwelcome calls and metered call dispute procedures. Information generated through the use of CCA/E and CLI facilities must be handled in accordance with Company Privacy Policy.

Also they do not deal with monitoring or interception for law enforcement purposes.

Finally, they do not deal with transactions involving payment of accounts by credit card over the telephone.

### 3. Policy

The Company has a Privacy Protection Policy containing ten principles. The Policy is at Attachment A. The following elements of that Policy are relevant to these voice monitoring or recording guidelines.

- Telecom Australia respects the rights of customers and the general community to privacy protection and accords highest priority to the protection of personal privacy alongside customer service.
- Our relationship with each customer, business and residential, is individual and private. To this end Telecom will abide by all provisions of statute law relating to telecommunications privacy matters. Telecom accepts the privacy principles set out in Federal legislation and commits

- We will vigorously defend the security of our telecommunications network and will take active technical and other steps to ensure the privacy of whoever uses it. Any monitoring of communications will be kept to an absolute minimum necessary to ensure the operation, maintenance or integrity of the network. Extended voice monitoring or voice recording for network maintenance operation purposes will only be undertaken with the consent of the customer.

#### 4. Legislation

The Telecommunications Interception Act contains restrictions on activities involving the listening to or monitoring of communications. Sub-section 6(1) of the Act defines an interception of a communication in the following way:

".....interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over the telecommunications system without the knowledge of the person making the communication."

Sub-section 7 of the Telecommunications Interception Act provides the following exceptions in respect of telecommunications interception:

- "Interception of a communication under a warrant", and
- "an act or thing done by an employee of the carrier in the course of his duties for or in connection with--
  - (i) the installation of any line or the installation of any equipment, used or intended for use in connection with the telecommunication service or the operation or maintenance of the telecommunication system;"
- "the interception of a communication of another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line".

The purpose of these exceptions is to allow employees of carriers to conduct the day to day business of the organisation. It is this area of activity to which these guidelines relate.

Any request for interception action from a law enforcement agency must be referred to the Corporate Secretariat, which will respond to such a request where a warrant has been properly issued. This includes any emergency requests made under section 30 of the Telecommunications (Interception) Act.

Procedures for dealing with unwelcome and life threatening calls are covered by Telecom's "Policy and Procedures for Unwelcome Calls".

## 5. Installation/Connection/Operation/Maintenance Activities

The legislative framework and the Company's policy position clearly anticipates that monitoring of customer lines is necessary for the purposes of conducting a telecommunications business. Monitoring is permitted for the purpose of ensuring that a connection has been made, that service quality is adequate and where it occurs incidentally in the operation, maintenance and installation, and or connection of equipment or a service, or a system.

It is the responsibility of Business Units to ensure that where monitoring occurs in these situations, that all elements of Company Privacy Policy and our legislative obligations are fully complied with. The elements that would need to be specifically covered include that any monitoring is either random or brief, such as that undertaken by a 1100 operator or from the test desk, and that any information obtained incidentally by such monitoring should not be retained nor disclosed by an employee.

Disclosure is also prohibited under section 88 of the Telecommunications Act 1991, subject to specific public interest exceptions, a breach which could attract a penalty of up to two years imprisonment.

Monitoring is conducted in connection with the IDD service in order to observe service quality. This monitoring which does not involve recording is consistent with ITU-T (CCITT) recommendation E.420 which recommends that administrations draw up a program for observation and tests designed for assessment of service quality. The procedures followed by the Company to observe service quality by observation of small segments of IDD calls is in accordance with ITU-T Recommendation E.422.

In relation to the Maritime service, there is 24 hour taping on all call and emergency frequencies. This procedure is performed at the request of the Australian Maritime Safety Authority as part of the requirements of the International Convention for Safety of Life at Sea. Tapes are retained for 30 days except where an incident has occurred in which case they may be retained for a longer period.

Calls to E000, the emergency service telephone number, are recorded by emergency service organisations.

Where there is any doubt in the mind of the staff member as to whether monitoring contemplated falls within the scope of this policy, the matter should be referred to the authorised officer relevant to your Business Unit.

## 6. Monitoring in Response to a Customer Complaint

These guidelines should be considered in conjunction with Telecom's policy on complaints handling.

In service complaints where faults are difficult to locate, it may be necessary to consider voice monitoring, and in some cases voice recording, of that customer's line.

It is Company policy that before voice monitoring takes place the customer's written consent must be obtained. That written consent must be obtained in the form shown at Attachment B. It is Company policy that any monitoring of this nature will be conducted by using aural observation (i.e. by a duly authorised staff member physically listening to a voice communication passing across the particular telecommunications system or line which is the subject of the complaint).

Where a staff member is considering voice monitoring, approval must first be obtained from the authorised employee as required in section 8 of this Guideline.

In addition, the privacy of the B parties, that is the party who is involved in telecommunication with the customer who's service is being investigated, must be observed. This means that in any monitoring situation the equipment used in that process must contain pip-tone as required by AUSTEL Technical Standards 5.9.3. In obtaining the initial consent from the customer it must be made clear to that customer that pip-tone will be used where monitoring takes place.

Where it has been decided to undertake voice monitoring, the authorised employee shall inform the exchange supervisor in writing that monitoring has been approved. The message shall include the time frame for the monitoring procedure. Upon completion of the monitoring the exchange supervisor must confirm in writing to the authorised officer that monitoring has concluded. Any further monitoring must be supported by a fresh authorisation.

Voice recording to assist in the diagnosis and substantiation of faults is not permitted except in the following circumstances:

If a customer specifically requests Telecom in writing to undertake voice recording to assist in the diagnosis or substantiation of faults, the matter should be raised with the Legal Directorate for consideration and formal recommendation. Voice recording may only be approved by written sign-off by the Chief Executive Officer, the Group Managing Director of the Commercial and Consumer Division or the Group Managing Director, Network and Technology, after receiving written advice from Telecom's Legal Directorate. Security arrangements (covering both physical and privacy aspects) to be applied in each case, the period of the recording and the identity of all officers proposed to have access to the recording will need to be documented and submitted as part of the approval process. Analysis of the recording will be confined to the approved technical analysis and no copies or transcripts of recorded information are permitted. On completion of analysis and within 30 days the tapes will be erased. At the customer's request, Telecom will hold the tapes up to 2 months for customer assessment of Telecom's analysis. Supervisory staff responsible for implementing approved recording arrangements are to ensure compliance with security and policy parameters approved in respect of monitoring arrangements.

The provisions of Section 88 of the Telecommunications Act 1991 prohibiting disclosure of information also apply in respect of voice monitoring and recording.

## **7. Equipment**

It is a requirement of these guidelines that any equipment used in the monitoring of a customer's service in accordance with Section 6, either by recording or by aural observation, must emit an audible pip-tone in accordance with the relevant AUSTEL Standard.

## **8. Authorised Employees**

The Group Managing Director of each Business Unit must, in their Business Unit authorisations, appoint a senior manager to approve individual monitoring requests. The appropriate manager is to ensure that Business Unit work practices and Business Unit instructions are consistent with Telecom's legal policy and ethical obligations in respect to voice monitoring activities.

In respect of voice recording, the approval of the Chief Executive Officer, the Group Managing Director of the Commercial and Consumer Division or the Group Managing Director, Network and Technology must be obtained in accordance with Section 6 of these guidelines.

## **9. Audit**

In accordance with the provision of Telecom's Privacy Protection Policy, the observance of these guidelines will be monitored by an independent audit process referred to in the Privacy Protection Policy. A yearly report on the audits conducted and the outcomes will be made available to the public. Customer privacy safeguards will be adhered to in the preparation of the reports.

## **10. Policy Coordination**

The Corporate Secretariat has responsibility for this Policy. Enquiries relating to the Policy should be directed to the Manager, Corporate Policy in the Corporate Secretariat. Enquiries on the application of privacy policy to Telecom products and services should be directed to Group Manager, Office of Customer Affairs in the first instance.



## PRIVACY PROTECTION - TELECOM POLICY

- 1: Telecom Australia respects the rights of customers and the general community to privacy protection and accords highest priority to the protection of personal privacy alongside customer service.
- 2: Our relationship with each customer, business and residential, is individual and private. To this end Telecom will abide by all provisions of statute law relating to telecommunications privacy matters and obligations arising out of any agreement with its customers. Telecom accepts the privacy principles set out in Federal legislation and commits itself to meet best international practice in this regard.
- 3: We will vigorously defend the security of our telecommunications network and will take active technical and other steps to ensure the privacy of whoever uses it. Any monitoring of communications will be kept to the absolute minimum necessary to ensure the maintenance or integrity of the network. Extended voice monitoring or voice recording for network operation and maintenance purposes will only be undertaken with the consent of the customer.
- 4: We will set clear restrictions on the amount and nature of information we ask from new or existing customers. We will allow such information to be used only for the purpose for which it was collected or to improve customer service.
- 5: We will not disclose information about our customers unless it is clearly in our customer's interest and with his or her consent. In common with most countries, Australian law requires telecommunications networks, subject to proper process, to supply specific information in cases of emergency, to help in the prevention or prosecution of crime and the handling of nuisance calls, and for some other reasons determined by the government. We will comply with such orders provided they are legal.
- 6: Telecom undertakes to take all steps that are reasonable in the circumstances to ensure that customer information is secure from any unauthorised access or disclosure.
- 7: We will give explicit consideration to any privacy issues that might be associated with the introduction of a new telecommunications service.
- 8: We will use our best endeavours to educate our customers about the possible privacy implications of any new telecommunications service that Telecom offers.
- 9: We recognise that wherever feasible customers should be permitted to choose among various degrees of privacy protection with respect to telecommunications services.
- 10: To ensure observance of this policy Telecom will institute a regular independent audit process reporting directly to the Chief Executive Officer. A yearly report on the audits conducted and their outcomes will be made available to the public.

### REQUEST TO UNDERTAKE CALL MONITORING

I request that Telecom monitor telephone calls made to or from my telephone service beginning on / / and ceasing on / /

I request that monitoring be conducted

- . Aurally\* or
- . Tape recorded.\*

I understand that:

Monitoring will only be undertaken between the dates specified and for the purpose of the detection and rectification of transmission faults.

A pip tone will be heard when call monitoring is being undertaken.

No information about the content of any calls monitored will be disclosed by a Telecom employee outside of Telecom. Tape recordings will be erased on completion of the testing process and within 30 days, unless I request their retention, for a period up to two months for assessment of Telecom's analysis.

Customer's Name .....  
(Please Print)

Signature ..... Date / /

Telephone Number (...)

\* Delete which ever is not applicable. It is Telecom policy that call monitoring should be conducted aurally by authorised staff within a telephone exchange unless a customer specifically requests that monitoring be carried out by tape recording.

.....  
*....Telecom Use Only*

Accepted

To.....

.....  
(Authorised employee)

Monitoring Completed

..... / /  
(Authorised employee)