The Senate

Legal and Constitutional Legislation Committee

Provisions of the Surveillance Devices Bill 2004

May 2004

ISBN 0 642 71402 9

Printed by the Senate Printing Unit, Parliament House, Canberra.

MEMBERS OF THE LEGISLATION COMMITTEE

Members

Senator Marise Payne, **Chair**, LP, NSW
Senator the Hon. Nick Bolkus, **Deputy Chair**, ALP, SA
Senator Brian Greig, AD, WA*
Senator Joseph Ludwig, ALP, QLD+
Senator Brett Mason, LP, QLD
Senator Nigel Scullion, CLP, NT

Substitute Member

* Senator Aden Ridgeway, AD, NSW to replace Senator Brian Greig for matters relating to the Indigenous Affairs portfolio

\+ Senator Kerry O'Brien, ALP, TAS to replace Senator Joseph Ludwig for matters relating to the Indigenous Affairs portfolio

Participating Members

Senator the Hon. Eric Abetz, LP, TAS	Senator Susan Knowles, LP, WA
Senator Mark Bishop, ALP, WA	Senator Meg Lees, APA, SA
Senator George Brandis, LP, QLD	Senator Ross Lightfoot, LP, WA
Senator Bob Brown, AG, TAS	Senator Sue Mackay, ALP, TAS©
Senator Kim Carr, ALP, VIC	Senator Julian McGauran, NPA, VIC
Senator Grant Chapman, LP, SA	Senator Jan McLucas, ALP, QLD
Senator Alan Eggleston, LP, WA	Senator Shayne Murphy, IND, TAS
Senator Christopher Evans, ALP, WA	Senator Kerry Nettle, AG, NSW
Senator the Hon. John Faulkner, ALP, NSW	Senator Robert Ray, ALP, VIC
Senator Alan Ferguson, LP, SA	Senator the Hon. Nick Sherry, ALP, TAS
Senator Jeannie Ferris, LP, SA	Senator Ursula Stephens, ALP, NSW
Senator Brian Harradine, IND, TAS	Senator Natasha Stott Despoja, AD, SA
Senator Leonard Harris, PHON, QLD	Senator Tsebin Tchen, LP, VIC
Senator Gary Humphries, LP, ACT	Senator John Tierney, LP, NSW
Senator Linda Kirk, ALP, SA	Senator John Watson, LP, TAS
Senator Andrew Bartlett, AD, QLD for matters relating to the Immigration and Multicultural Affairs portfolio.	

Secretariat

Mr Jonathan Curtis	Secretary
Ms Anne O'Connell	Principal Research Officer
Ms Barbara Rogers	Executive Assistant

Suite S1.61
Parliament House

Telephone: (02) 6277 3560
Fax: (02) 6277 5794
E-mail: legcon.sen@aph.gov.au

TABLE OF CONTENTS

Chapter 1

Introduction

1.1 On 31 March 2004 the Senate referred the Surveillance Devices Bill 2004 to the Legal and Constitutional Legislation Committee for inquiry and report by 27 May 2004.

Key provisions of the Bill

1.2 The Bill has three main purposes:

- To establish procedures for Law Enforcement Officers (LEOs) to obtain surveillance device warrants, emergency authorisations or tracking device authorisations for use in:
    - criminal matters; and
    - the location and safe recovery of children who are the subject of recovery orders under the Family Law Act 1975.
- To restrict the use, communication and publication or information obtained through surveillance devices or connected with them.
- To provide for the secure storage and destruction of the information obtained through surveillance devices, and also to impose requirements for masking reports in connection with the surveillance device operations (clauses 3(a)(b) and (c) of the Bill)

1.3 The Bill does not include provision for surveillance by telecommunications devices, which are covered by the Telecommunications (Interception) Act 1979 ('The TI Act').

Conduct of the Inquiry

1.4 The Committee wrote to a number of interested individuals and organisations inviting submissions by 23 April 2004. The details of the Inquiry, the Bill and associated documents were also placed on the Committee's website.

1.5 The Committee received 6 Submissions which are listed in Appendix 1. The submissions were also placed on the Committee's website for public access.

1.6 The Committee held a public hearing in Canberra on May 10 2004. A list of witnesses appears at Appendix 2 , and copies of the Hansard are available through the internet at http://aph.gov.au/hansard

Acknowledgement

1.7 The Committee thanks those organisations and individuals who made submissions and gave evidence at the public hearing.

Notes on references

1.8 References in this report are to individual submissions as received by the Committee, not to a bound volume. References to the Committee Hansard are to the proof Hansard: page numbers may vary between the proof and the official Hansard transcript.

Chapter 2

Background

2.1 This chapter outlines the background and main provisions of the Bill.

Introduction

Current process for obtaining and using a surveillance device

2.2 The Committee notes that there is at present no legislation at the Commonwealth level which regulates the use of all surveillance devices. The Committee was advised that there has been a power available to law enforcement agencies under the *Customs Act 1958,* and the *Australian Federal Police Act 1979* to use listening devices, and for telecommunications devices under the *Telecommunications (Interception) Act 1979*.[1]

2.3 The use of these devices is subject to an application for a warrant in which the applicant must explain to the satisfaction of the Judge or AAT member considering the application, why the warrant is required and the circumstances in which it will be used.

2.4 The Committee notes there has been no Commonwealth legislation governing the use of optical devices or tracking devices, although some of these are regulated in some States. For example, in New South Wales, South Australia, Western Australia and Queensland there is legislation which applies to listening devices, optical devices and tracking devices.[2] In addition to these devices, the Victoria and the Northern Territory legislation also regulates data surveillance devices,[3] while in Tasmania and the ACT the legislation applies only to listening devices.[4]

The Working party

2.5 In 2002, the Prime Minister and State and Territory leaders agreed on a number of reforms to 'enhance arrangements' for dealing with multi-jurisdictional

---

1 *Committee Hansard*, 10 May 2004, p. 3.

2 *Listening Devices Act 1984* (NSW); *Listening Devices Act 1972* (SA); *Surveillance Devices Act 1998* (WA); *Police Powers & Responsibilities Act 2000* (QLD).

3 *Surveillance Devices Act 1999* (VIC); *Surveillance Devices Act 2000* (NT).

4 *Listening Devices Act 1991* (TAS); *Listening Devices Act 1992* (ACT), *Australian Federal Police Act 1979* (Cth).

crime. As part of these reforms, they agreed to introduce model laws for a national set of powers for cross-border investigations covering electronic surveillance devices.[5]

2.6 The task of developing these model laws was given to the national Joint Working Group established by the Standing Committee of Attorney's-General and the Australian Police Ministers Council (the JWG). The JWG published a discussion paper in February 2003[6] (the Discussion Paper), and following this, a report in November 2003 (the Report), which incorporated the electronic surveillance model bill.[7] The Bill is based on this model bill.

2.7 The Report identified gaps in the existing legislative regime governing the use of surveillance devices by law enforcement agencies, and noted that there is no comprehensive legislative regime governing the use of surveillance devices by law enforcement in Australia, apart from the TI Act's regulation of telecommunications interception.[8] It further noted that the current legislation does not contain mutual recognition of provisions that allow surveillance device warrants issued in one State to be recognised in another.[9]

2.8 The report also noted that the increase in cross-border criminal activity demands strategies which can respond without the undue delays and potential loss of evidence imposed by a need to obtain warrants in every State or Territory entered by a criminal suspect.[10]

State / Federal law enforcement issues

2.9 Because there is no uniform Commonwealth regime regulating the use of listening devices, the AFP are limited in their use of surveillance devices, to what is permitted under Commonwealth laws, and in the absence of such laws, they are subject to the limitations of local State and Territory laws and the common law. However, unlike State and Territory police, they are unable to use the local warrant regimes.

---

5 *Cross-border investigative powers for law enforcement*, Report of the Standing Committee of Attorneys General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, November 2003. p.i.

6 *Cross-border investigative powers for law enforcement*, Discussion Paper. The Standing Committee of Attorneys General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, February 2003.

7 *Cross-border investigative powers for law enforcement*, Report of the Standing Committee of Attorneys General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, November 2003.

8 *Cross-border investigative powers for law enforcement*, Report of the Standing Committee of Attorneys General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, November 2003. p.345

9 Ibid.

10 *Cross-border investigative powers for law enforcement*, op cit, p.345

2.10 Under Commonwealth law, there are very limited examples of powers where surveillance devices can be used. These include the *Customs Act 1901*, which allows the use of listening devices in investigating narcotics offences, and the *Australian Federal Police Act 1979* which allows the use of listening devices in the investigation of other Commonwealth offences or serious offences against the law of the Australian Capital Territory.[11]

2.11 If the Bill were enacted, the AFP would be able to rely on a uniform Commonwealth regime to allow it to use surveillance devices in all Commonwealth investigations. It is proposed that the model bill will be adopted by all States and territories. If this is to eventuate, having similar regimes for the use of surveillance devices would simplify the investigation of both Commonwealth and State and Territory offences.

Provisions of the Bill

2.12 The Bill is divided into 7 parts and a Schedule providing consequential amendment of other Acts. The legislation will commence on assent.

What is authorised by the Bill?

2.13 The Bill authorises a process for the use of a variety of surveillance devices. A surveillance device is defined in clause 6 of the Bill as:

- a data surveillance device – equipment capable of recording or monitoring data entered into, or received by, a computer on an ongoing basis;
- a listening device – devices which monitor and record audio emissions in the open air;
- an optical surveillance device – cameras, video recorders and other devices which allow the viewing and recording of images;
- a tracking device – devices which emit a radio signal to monitor the movement of a vehicle or object to which the device is attached;
- a combination of any 2 of the above; or
- a device of a kind prescribed by the regulations.

2.14 The process results in the issue of a warrant authorising the applicant or a person on his or her behalf to install surveillance devices on property designated in the warrant. Property includes a motor vehicle.

2.15 A warrant is a document issued by an authorised person to do something in the course of law enforcement which would ordinarily not be permitted. The most commonly recognised kind of warrant is the search warrant (issued in the Commonwealth under section 3E of the *Crimes Act 1914*) which allows entry onto

11 *Cross-border investigative powers for law enforcement* Discussion Paper, op cit, p.203.

premises where the applicant reasonably suspects that there are items connected with a crime.

2.16 The warrants which are proposed under the Bill allow entry onto premises to install surveillance devices, including listening devices and tracking devices. Two types of warrant are authorised under clause 10:

- a surveillance device warrant, and
- a retrieval warrant.

2.17 The surveillance device warrant allows the applicant or his or her representative to enter premises and install the device, and the retrieval warrant allows entry to retrieve the device.

2.18 The legislation also provides for the issue of emergency warrants as well as providing for the use of some devices without a warrant. The warrants are covert in their execution, and the process includes compliance and monitoring requirements which are outlined below.

Who may apply for a surveillance device warrant?

2.19 Applications for a warrant are made by an LEO or another person on his or her behalf (clause 14). The definition of law enforcement officer is broad:

> (a) in relation to the Australian Federal Police – the Commissioner of Police, a Deputy Commissioner of Police, any AFP employee, any special member or any person who is seconded to the Australian Federal Police; or
>
> (b) in relation to the Australian Crime Commission – the Chief Executive Officer of the Australian Crime Commission or any other person who is covered by a paragraph of the definition of member of the staff of the ACC in section 4 of the *Australian Crime Commission Act 2002*; or
>
> (c) an officer (however described) of the police force of a State or Territory or any person who is seconded to that police force.

What offences may a warrant be issued for?

2.20 Clause 6 of the Bill defines a relevant offence as:

- Commonwealth offences and State offences with a federal aspect which attract a maximum custodial penalty of 3 years or more;
- offences under section 15 or 18 of the *Financial Transaction Reports Act 1988*; and
- offences under certain sections of the *Fisheries Management Act 1991* or an offence prescribed by the regulations.

2.21 State or Territory LEOs may make an application for a surveillance device for a relevant offence, but not for a State offence which has a federal aspect. The

Explanatory Memorandum notes that clause 7 establishes that a State offence has a federal aspect if:

- the Commonwealth could have enacted a valid provision covering a State offence, or the specific conduct involved in committing that offence;
- the investigation of a State offence is ancillary to the AFP's investigation of a Commonwealth or Territory offence.

Applications

2.22 An application for a surveillance device warrant can be made if the law enforcement officer suspects on reasonable grounds that:

- a relevant offence is being/is about to be/has been committed, and an investigation conducted; and
- the use of a surveillance device is necessary to obtain evidence relating to the suspected offence.

Applications without affidavit

2.23 The Bill contemplates situations where in an extreme emergency the application to a Judge or AAT member may not be supported by an affidavit, and allows for the affidavit in support to be provided up to 72 hours after the making of the application 'whether or not a warrant has been issued'.[12]

2.24 Clause 15 provides for remote applications to be made by telephone, fax, email 'or any other means of communication'.

Who may issue a warrant?

2.25 Warrants may only be issued by an eligible Judge or a nominated AAT member. An eligible judge is a Judge of a Court created by the Parliament (for example, the Federal Court or the Family Court) who has consented in writing to be declared eligible by the Minister.

2.26 The nominated AAT members may include the Deputy President, full and part time senior members or a member, although the last two cannot be appointed unless they have been admitted as a legal practitioner for at least five years. The appointment ceases if the person ceases to be a member of the AAT.

Requirements for issuing a warrant

2.27 Subclause 16 (1) of the bill indicates that the issuing judge or AAT member must be satisfied:

12 subclauses 14(5) and (6)

- that there are reasonable grounds for the suspicion on which the warrant is based;
- that where the warrant relates to a recovery order – that there is an actual order in existence;
- where an application is unsworn, it was impracticable for an affidavit to be made available with the application; or
- in the case of a remote application, that it would have been impracticable for the application to have been made in person.

2.28 In deciding whether to grant the application, the Judge or member must have regard to a number of matters, including the extent to which the privacy of any person is likely to be affected, the probable value of any intelligence obtained, and whether or not there was any alternate means of obtaining it.

2.29 The Act appears to contemplate – except for remote applications – the personal attendance of the applicant and there would appear to be no impediment to the applicant providing under oath, oral material in support of the application.

The Warrant

2.30 The warrant must contain the information specified in clause 17. This includes:

- a Statement by the issuing judge to the effect that he or she considered the matters in subclause 16(1) (see above) as well as having regard to the matters in 16(2);
- the name of the applicant and the offences or the recovery order to which the warrant relates;
- the duration of the warrant (no longer than 60 days);
- details of the premises, the category of the device to be used, the identity of any person whose activities are to be observed (and if not known, the fact that the identity is not known):
- any particular conditions for use of the device; and
- the name of the officer responsible for executing the warrant, and any other conditions for executing the warrant.

2.31 Other features of the warrant include:

- The ability to retrieve the device after it ceases to be required. If this occurs within the life of the warrant (up to 90 days) it is unnecessary to reapply for a warrant to retrieve it; however if the warrant has expired, a retrieval warrant is

necessary [13]and is issued under similar requirements and constraints as a surveillance warrant.

- The ability to extend or vary the warrant,[14] and also to revoke it.[15] Warrants may be revoked by the issuing Judge or member or in some circumstances by the chief officer of the law enforcement agency to whom the warrant is granted. The chief officer may only revoke where the device was sought by an LEO from the same agency, and where the chief officer is satisfied the device is no longer required.[16] Retrieval warrants may also be revoked.[17]

Part 3 – Emergency Authorisations

2.32 Part 3 of the Bill allows emergency authorisation of the use of a surveillance device by an 'appropriate authorising officer'. This person is defined in clause 6 of the Bill and includes Commissioners of Police and senior AFP employees, and their equivalent in the Australian Crime Commission, and State and Territory Police forces.

2.33 Emergency authorisations may be given under the circumstances described in cl.28 which include:

- imminent serious and urgent risk of serious violence to a person or substantial property damage exists, and a surveillance device is necessary to deal with that risk; and
- that it is not practicable to apply for a surveillance device warrant.

2.34 Similar requirements apply to circumstances involving recovery orders.

2.35 The authorising officer must be satisfied that there are reasonable grounds founding the suspicion giving rise to the need for the application.

2.36 Clause 30(1) also provides for specific offences and circumstances for emergency authorisation where evidence may be lost. These include customs and drug offences, as well offences under the *Criminal Code Act 1995* such as terrorism, people smuggling, and offences involving sexual servitude.

2.37 The warrant must be considered retrospectively within two business days after the emergency authorisation.[18] If the Judge or member does not issue the warrant, the devices installed under the emergency approval must be withdrawn.

---

13 See Division 3, clause 22.

14 Clause 19

15 Clause 20

16 Clause 21

17 Clause 27

18 Subclause 33(1)

Use of evidence obtained under emergency authorisation.

2.38 Evidence obtained under an emergency authorisation is not inadmissible merely because it was obtained before an approval was given[19] although there may be other reasons for it not to be admitted. Where emergency approval has been withheld, it may still be possible to use the evidence in some cases, as a presiding justice can exercise his or her discretion to admit evidence improperly obtained under section 138 of the *Evidence Act 1995* (Cth) or section 138 of the *Evidence Act 1995* (NSW).

Part 4 – Use of certain devices without warrant

Optical surveillance devices / Listening and recording devices

2.39 The use of optical surveillance devices or devices for listening to, or recording words spoken by a person is permitted where there is no need either for entry on to premises without permission, or interference without permission with any vehicle or thing. This is subject to the purpose being within the functions of the AFP if it is the AFP seeking to use the device, or the ACC if it is the ACC using it.

2.40 Similarly, State or Territory LEOs may also use these devices without a warrant but similar constraints apply as for the application for a warrant.

Tracking devices

2.41 Unlike the optical, listening and recording devices referred to in clauses 37 and 38, use of tracking devices without a warrant requires the approval of an authorising officer in writing.[20] The use of these devices is limited to circumstances in which there is no interference without permission with premises or vehicles or things.[21] An application must contain similar information as would be required for a warrant, and the authorising officer is required to keep a written record of the authorisation.[22]

Part 5 – Extraterritorial operation of warrants

2.42 Under clause 42, surveillance warrants can be issued for use in a foreign country, or on a vessel or aircraft registered in a foreign country, provided the appropriate consent has been given from that country.

2.43 There are requirements which attach to the surveillance process, including advising the Minister in writing that it has been agreed to by the foreign country.

---

19 Clause 36

20 Clause 39

21 Subclause 39(8)

22 Clause 40

2.44 However, for offences under the *Fisheries Management Act 1991* involving a foreign registered vessel in waters within the outer limits of the Australian fishing zone, there is no consent requirement.

Part 6 – Compliance and monitoring.

Division 1 – Protection of surveillance device technologies and methods

2.45 Clause 45 sets out the offences and penalties for unlawfully using, recording publishing or communicating information under this legislation. There is an aggravated offence attracting a maximum custodial penalty of 10 years where such use endangers a person or prejudices the effective conduct of an investigation.[23] There are limited conditions under which protected information can be used.[24]

2.46 There are also provisions for the secure keeping of surveillance device records,[25] and for the protection of the methods and technologies of surveillance.[26]

Division 2 – Reporting and record-keeping

2.47 The Bill requires records to be kept of the results of the warrant, including whether or not it was executed, and if so, what the outcome was. Clause 53 requires the chief officer of a law enforcement agency to keep a comprehensive register of the warrants, emergency authorisations and TD authorisations.

2.48 Clause 49 provides that the Minister must receive a report on each warrant or authorisation as well as a copy of the warrant and associated documents. Under clause 50, the relevant agency must also provide an annual report to the Minister which includes an account of the outcomes in matters where the warrants were sought.

Division 3 – Inspections

2.49 The Ombudsman or delegate is required to inspect the records of a law enforcement agency to determine the extent of compliance with the Act.[27] The Ombudsman has considerable powers to require attendance by any applicant for an SD warrant, to give information relevant to an inspection.[28]

2.50 The Ombudsman is to be given information and access to information, despite any other law.[29] The Ombudsman may also receive from, and give to State or

---

23 Subclause 45(2)

24 Subclause 45(5)

25 Clause 46

26 Clause 47

27 Clause 55

28 Clause 56

29 Clause 57

Territory agencies or inspecting authorities, information obtained under the proposed legislation in appropriate circumstances.[30]

2.51 Clause 61 requires:

- the Ombudsman to report every 6 months in writing to the Minister on each inspection under clause 54; and
- within 15 sitting days of the receipt of the report, the Minister to table a copy of that report in each House of the Parliament.

Division 4 – General

2.52 Clause 62 provides for evidentiary certificates to be issued about things done in the execution of a warrant, including the provision of technical advice, or in connection with an emergency or TD authorisation.

Similarities to other legislation

Telecommunications interception regime

2.53 The Bill seeks to regulate the use of surveillance devices by law enforcement, and as a result raises similar privacy and civil liberty issues as those raised in the operation of the TI Act. There are two significant differences between the TI Act and the Bill, which are the class of persons who may apply for a warrant, and the absence of a formal civil remedy process for those subject to an unlawful use of a surveillance device.

2.54 The class of persons entitled to apply for a surveillance device warrant is wider under the proposed legislation than it is under the TI Act. For example, under the TI Act, a member of the AFP may make an application on behalf of the AFP, but an employee of the AFP is not named as being able to do so, as it is in the Bill.

2.55 Similarly, under the TI Act, in the case of the ACC it is the CEO, an examiner or a staff member who is also a member of a police force who may apply for a TI warrant. Under the Bill staff members however described are eligible to seek warrants.

2.56 Another difference between the Bill and the TI Act is that under the TI Act there is a formal civil remedies process available for those who are subjected to unlawful interception,[31] whereas there is no equivalent protection or remedy under the Bill.

State and Territory legislation

30 Clause 58

31 Section 107A *Telecommunications (Interception) Act 1979*

2.57 It is envisaged that all States and territories will enact equivalent legislation based on the model bill. The current legislation in some States and territories regarding the use of surveillance devices is considerably different to the model bill, and some jurisdictions do not regulate certain types of device.

2.58 In Tasmania and the ACT regulation applies to listening devices only.[32] The duration of warrants is 60 days in Tasmania.[33]

2.59 In New South Wales, South Australia, Western Australia and Queensland the legislation applies to listening devices, optical devices and tracking devices.[34] The duration of warrants is 90 days for South Australia and Western Australia, 30 days in Queensland, and 21 days in New South Wales.[35]

2.60 Victoria and the Northern Territory regulate the use of listening devices, optical surveillance devices, tracking devices, and data surveillance devices.[36] In Victoria warrants are for 90 days, and 21 days in the Northern Territory.[37]

---

32 *Listening Devices Act 1991* (TAS); *Listening Devices Act 1992* (ACT), *Australian Federal Police Act 1979* (Cth).

33 Paragraph 17(4)(c) *Listening Devices Act 1991* (TAS)

34 *Listening Devices Act 1984* (NSW); *Listening Devices Act 1972* (SA); *Surveillance Devices Act 1998* (WA); *Police Powers & Responsibilities Act 2000* (QLD).

35 21 days plus 10 days retrieval time paragraph 16(4)(c) *Listening Devices Act 1984* (NSW), up to 21 days retrieval time upon application to Judge, ss 16A(3)(4); .ss 6(7) *Listening Devices Act 1972* (SA); ss 19(4) *Surveillance Devices Act 1998* (WA); ss 68(17) *Police Powers & Responsibilities Act 2000* (QLD).

36 *Surveillance Devices Act 1999* (VIC); *Surveillance Devices Act 2000* (NT).

37 sub-paragraph 17(3)(c)(ii), paragraph 17(5)(a) *Surveillance Devices Act 1999* (VIC); paragraph 9(5)(d) *Surveillance Devices Act 2000* (NT).

CHAPTER 3

Issues arising from the Bill

Introduction

3.1 This chapter covers two principal issues surrounding the introduction of this legislation. Firstly, why is the bill necessary, and secondly, how appropriately does the bill meet the identified requirement. The latter issue includes consideration of a number of more technical legal issues such as the process for authorisation of the use of surveillance devices, especially in circumstances where no warrant is required, together with the security and destruction of records of information collected using surveillance devices.

Why is the bill necessary?

3.2 The proposed legislation has two principal rationales.

3.3 The first is that there is presently no Commonwealth legislation which regulates the use of data surveillance devices, tracking devices or optical surveillance devices. The only existing legislation covering surveillance devices relates to listening devices, under Part II Division 2 of the *Australian Federal Police Act 1979* and Part XII Division 1A of the *Customs Act 1901*, and telephone interception under the *Telecommunications (Interception) Act 1979*.

3.4 The gaps in the current regulatory regime reflect a variety of new technologies that have become available to law enforcement agencies in recent years. As such, the Attorney General told Parliament that the law on surveillance devices needed to be updated 'to meet the demands of 21st century policing'.[1]

3.5 The issues surrounding the need for this legislation were comprehensively explored in a discussion paper and subsequent report which was produced by the Standing Committee of Attorneys General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers in April and November 2003 respectively. The paper noted that the use of surveillance devices by Commonwealth State and Territory law enforcement agencies is regulated by a combination of divergent legislation and the common law.[2] The concerns about the Commonwealth State and territory legislation identified by the working party as inhibiting effective law enforcement across Australia's internal borders included:

- the types of devices covered;

---

1 *House of Representatives Hansard*, 24 April 2004, p.27010

2 *Cross-border Investigative Powers for Law Enforcement* Discussion paper of the Standing Committee of Attorneys General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers February 2003 p. 201

- the issuing of warrants;
- the offence threshold for warrants to be sought;
- the duration of warrants;
- the powers that may be exercised under a warrant; and
- the reporting and accountability requirements associated with warrants.[3]

3.6 The Working Party further observed that the current legislation does not contain mutual recognition provisions which allow surveillance device warrants to be issued in one State and recognised in another. A model bill was drafted which forms the basis for this Commonwealth bill but it differs from the model bill in some respects.

3.7 The Australian Crime Commission (ACC) and the Australian Federal Police (AFP) both provided submissions and evidence to the Committee. They were also concerned about the lack of a nationally consistent regime for obtaining and using surveillance devices. The bill also includes provisions for the use of surveillance devices outside Australia in some circumstances.

3.8 In some states some surveillance devices are regulated under state law: this bill provides a framework for the authorisation of surveillance devices and their use by law enforcement officers in Commonwealth matters as well as those which involve the states and the Commonwealth.

3.9 The inconsistencies between States and Territories legislation in this area inhibit the cross border activities which are made necessary by multi jurisdictional criminal activity. The AFP submission indicates:

> The success of the AFP in bringing to justice those involved in the commission of serious crimes … depends on available tools of investigation, information gathering capabilities and the admissibility of that information in proceedings in Australian Courts.[4]

3.10 The AFP also notes that the bill seeks to 'consolidate and update the regulatory regime for the use of surveillance devices by Commonwealth Agencies.'[5]

3.11 In evidence the ACC told the Committee that the standardisation and the regulation of all the surveillance methods would alleviate operational and evidentiary difficulties. These included the potential loss of evidence and intelligence. The ACC continued:

---

3 *Cross-border Investigative Powers for Law Enforcement*, Report of the Standing Committee of Attorneys General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers November 2003 p.345

4 Submission 5, p.3

5 Submission 5, p.1

> For example, if there is an opportunity to introduce an undercover operative into a meeting, that opportunity may come at any time … we might need to record its audio and we might need to video it, to obtain images from that meeting. We need to be able to do that straight away. We have not got time to really think about it, otherwise the opportunity is lost.[6]

3.12 The Committee also notes that in some instances it is necessary for Commonwealth officers to obtain separate warrants, for example, for listening devices, if a matter crosses state borders. Administratively and operationally, this can cause delays and as indicated by the ACC, the loss of evidence.

3.13 In evidence to the Committee the Attorney General's Department explained the Commonwealth's overall position:

> … the Commonwealth has sought, in seeking to achieve a greater measure of uniformity than currently exists, to work with the model legislation to develop something that would be suitable for Commonwealth investigative regimes.[7]

Need for balance – law enforcement and privacy

3.14 As always, these considerations must be balanced against the need to protect the privacy of individuals, whose personal lives will be investigated, recorded and stored by law enforcement officials. An important part of this consideration is also the fact that it is not only those who are under investigation who will be subject to this surveillance, but also the wide range of individuals who have private and official dealings with them.

3.15 To varying degrees witnesses and submitters accepted that in principle, surveillance powers are 'a necessary evil.' However, there were reservations expressed in a number of submissions.[8] Mr David Bernie, representing the Council for Civil Liberties, told the Committee:

> Our concerns are general concerns … we are concerned obviously about further increasing surveillance over Australian citizens but recognise, of course that with the technology that is becoming available law enforcement authorities are going to want to use such technology … it is best that it be regulated by some sort of legislation like this. … we think it is important that there be as much control over that outside the executive as is practically possible.[9]

3.16 The range of views indicates that there is not only concern about keeping information confidential, there is also concern about general availability of the

---

6 *Committee Hansard,* 10 May 2004, p. 6.

7 *Committee Hansard,* 10 May 2004 p. 28

8 Submissions 1,3,4,6,

9 *Committee Hansard*, 10 May 2004, p. 11

information, and its transparency. These issues are considered in the context of privacy rights.

No common law right to privacy

3.17 An important underlying consideration in assessing the implications of the bill is that there is no underlying right at common law to privacy. Existing statutory provisions that protect aspects of privacy[10] create general privacy principles and require collecting agencies to prevent improper disclosure or use of personal information. Nevertheless, this does not amount to a coherent universal right to privacy.

3.18 Mr David Bernie, Vice President of the NSW Council for Civil Liberties explained the Australian situation and contrasted it with the US tort of invasion of privacy.[11] Mr Bernie said:

> As I understand it, US Supreme Court decisions about right to privacy have certainly been used to strike down, for instance, criminal laws which were considered to infringe that area.[12]

3.19 The Committee notes that the US example also operates in the context of a 'litigation friendly' environment; however the existence of a statutory right to privacy was canvassed in evidence by Mr Paul Chadwick, the Victorian Privacy Commissioner.

3.20 Mr Chadwick suggested that bills such as this should have a clause in the objects section which includes respect for privacy, which he noted would be consistent with Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

3.21 In response, the Attorney General's Department told the Committee that:

> the legislation in paragraph 16(2)(c) specifically requires the court to consider the privacy implications of granting a warrant before it actually approves the granting of a warrant. While privacy concerns are not addressed in the objects clause, they are clearly required to be taken into account before a warrant is issued.[13]

3.22 There is very fine balance between maintaining and protecting the privacy of individuals on the one hand, and the wider public interest of obtaining evidence with which to prosecute and convict serious offenders. It is also likely that this dilemma will become of increasing significance with the rapidly growing potential for intrusive technological surveillance.

---

10 Contained in the *Privacy Act* (Cth) 1988

11 *Committee Hansard*, 10 May 2004, p. 15

12 *Committee Hansard,* 10 May 2004, p. 17

13 *Committee Hansard,* 10 May 2004, p. 30

3.23 In these circumstances, privacy must also be taken in a wider context. The Victorian Privacy Commissioner told the Committee that privacy must extend beyond just the act which may invade privacy; but also to the use of the surveillance product, and the security of that product. He told the Committee:

> it is not just about the uses to which the state might put that [information]; it is about whether the state secures it when it is in its custody and whether it is of accurate quality, especially where the state purports to take decisions adverse to the individual on the basis of that data.[14]

Conclusion

3.24 Overall, the need for this bill was recognised by witnesses to the inquiry. Organisations with a public interest focus such as the Victorian Privacy Commissioner told the Committee:

> the powers are necessary, although we all feel uneasy about them; and the potential for abuse is real.[15]

3.25 Similarly, the Deputy President of the NSW Council for Civil Liberties also accepted the need for the legislation, albeit with controls. He told the Committee:

> with the technology that is becoming available law enforcement authorities are going to want to use such technology and so it is best that it be regulated by some sort of legislation like this. In approaching that, we think it is important that there be as much control over that outside the executive as is practically possible.[16]

3.26 The Committee therefore **concludes** that the powers proposed in the bill are necessary, but has some reservations about aspects of the proposed bill, and its ability to balance privacy and accountability concerns with fulfilling its objectives. These issues are discussed below.

Major Issues

3.27 Key concerns arising from the bill relate chiefly to four issues surrounding the issuing of a warrant, as well as the adequacy of controls over the storage use and destruction of information resulting from the surveillance.

3.28 The Committee also considered the effectiveness of the accountability mechanisms contained in the proposed scheme.

---

14 *Committee Hansard*, 10 May 2004, p. 20

15 *Committee Hansard,* 10 May 2004, p. 19

16 *Committee Hansard,* 10 May 2004, p. 11

Emergency warrants

3.29 As noted in chapter 2, the bill provides that in applying for a warrant the applicant must satisfy the Judge or AAT member of a number of conditions, and in considering the application, the Judge or member must also have regard to issues such as the extent to which the privacy of a person might be affected. The bill allows for remote applications by telephone, fax, email or any other means of communication. This is consistent with similar legislation.

3.30 However, there is a third method of application which allows emergency authorisation of the use of a surveillance device by an 'appropriate authorising officer'. This person is defined in clause 6 of the bill and includes Commissioners of Police and senior AFP employees, and their equivalent in the Australian Crime Commission, and State and Territory Police forces.

3.31 Any emergency authorisation must be referred to a Judge within two business days, and if it is refused, the devices must be withdrawn. Any evidence obtained under these circumstances may not be used in evidence under clause 45(3). Emergency authorisations are limited to situations in which there are serious circumstances – for example, a serious risk to a person or substantial risk to property, or where a recovery order is in force.

3.32 While the Committee is sympathetic to the demands made of law enforcement officers in the field, it has concerns about the use of a potentially invasive device in the absence of an affidavit or considered application. This is notwithstanding the subsequent granting of the warrant after the event.

3.33 It also came to the Committee's attention, that there is potential for the emergency warrant to remain in force unapproved for up to four days – for example, when a warrant is issued late on a Friday, the application for approval does not have to be finalised until two business days have elapsed. [17]

3.34 In contrast, the Committee noted that under the TI Act the time within which action must be taken is 24 hours.

3.35 The Committee accepts the need for the granting of emergency warrants but stresses that these must be subject to strict controls. The Committee also concedes that there may be valid operational reasons to justify allowing two days rather than one in which to obtain approval. However, with authorised personnel available on duty around the clock, the Committee considers that 48 hours is sufficient for the application to be made.

Recommendation 1

17 *Committee Hansard*, 10 May 2004, p.29

3.36 The Committee recommends that the time allowed in clause 33 of the bill relating to emergency applications to a Judge or Member be amended from two working days to 48 hours.

Warrant not required

3.37 The bill provides that the use of optical surveillance devices which can include commonplace items such as binoculars or cameras, do not require a warrant or authorisation. This is provided under Part 4 of the bill and applies:

> **37(1)**
>
> … if the use of that device does not involve:
>
> (c) entry onto premises without permission; or
>
> (d) interference without permission with any vehicle or thing.

3.38 In his second reading speech for the bill, the Attorney General suggests that the purpose of this is to permit the use by police of binoculars without the need for a warrant. However, the definition of 'optical surveillance device' makes it clear that visual recording as well as visual observation without a warrant would be permitted by this subsection. This includes still or video cameras using conventional lenses, light intensification, thermal and infrared.[18]

3.39 The AFP told the Committee that this type of surveillance in a public area is at the lowest end of interference with privacy, and should not require a warrant.[19] While the Committee accepts that while the surveillance involved does pose some potential for breaching privacy, the potential is low relative to the operational implications of seeking authorisation for the use of optical surveillance devices which would impede the progress of investigations to an unacceptable level.

Protection against misuse

3.40 Part 6 of the bill sets out requirements for the protection of information obtained under a warrant as well as information obtained without a warrant when there should have been one. However, this implies that information gained in circumstances that do not require a warrant (such as those outlined above) do not receive any such protection. The Committee raised this with the Australian Crime Commission who told the hearing:

> The physical surveillance team's task is recorded on an official tasking form and that is tasked by the head of the investigation, so the physical surveillance cannot just run off at a whim and just decide to follow somebody or carry out surveillance. So they are tasked by the head of the investigation. During the course of surveillance they prepare running sheets which are contemporaneous notes which are treated as highly protected

18 Submission 5A

19 *Committee Hansard*, 10 May 2004, p.24

> documents and those sorts of notes can become documents of the court and admitted into evidence.[20]

3.41 The Committee was also advised that these notes are not subject to any kind of oversight nor are they reviewed by the Ombudsman.

3.42 While the Committee accepts that there are internal restraints on the activities of the surveillance teams, it remains concerned that there is no codified protections for the use of information gained through such surveillance, or consideration given to the consequences of its use, or misuse. Consequently, the Committee concludes that there is a need for both explicit protection of this information as well as the need to keep records of the surveillance which should be accessible to the Ombudsman.

Recommendation 2

3.43 The Committee recommends that the legislation be amended to include a requirement for the Ombudsman to review (along with warrant records) the records of the use of optical surveillance devices.

More than one type of warrant: warrant-shopping?

3.44 Electronic Frontiers Australia (EFA) focussed its comment on the data surveillance device provisions of the bill, which allow the use of equipment capable of recording or monitoring data entered into, or received by, a computer on an ongoing basis. EFA's concerns centred on the possibility that these provisions could effectively remove the need for law enforcement agencies to obtain warrants under the TI Act. EFA said:

> A data surveillance warrant could be used to covertly install software or hardware in a computer. Such a device could record all information entered into the computer before it passes over a telecommunications system thereby obviating the need for a TI warrant because the information is not passing over the telecommunications system at the time it is being recorded.[21]

3.45 While the Bill indicates that it does not authorise anything for which a warrant would be required under the TI Act, EFA has little confidence in this as there are still aspects of that Act which are unclear – particularly in defining where a telecommunications system begins and ends. EFA also point to varying inter-agency views about the parameters which should be drawn around the TI Act.[22]

3.46 The Committee is concerned at this apparent overlap between the bill and other legislation, notably the TI Act, which could result in unauthorised access to confidential information.

---

20 *Committee Hansard,* 10 May 2004, p.8

21 Submission 6, p.2

22 Ibid.

3.47 This reflects a more general concern that the addition of the regime proposed by the Surveillance Devices Bill could result in something of an operational smorgasbord, allowing Law Enforcement Agencies (LEAs) to exploit vague areas or inconsistencies in the legislation to pick a warrant – be it a TI warrant, surveillance device warrant or a search warrant – that enabled them to do what they want. The ACC was asked what would stop an agency from making a range of applications to see which was successful.

3.48 The ACC responded:

> There is nothing to stop an agency from going warrant shopping except that you need to be able to resource these things. The installation of a listening device is a very lengthy process. … People need to be able to do it covertly, without being detected. We need to be able to service that device if something happens to it. … It regulates itself and the ACC, like everybody else, does not have the resources to put about the place, so we must be very strategic in how we deploy this kind of methodology in our investigation.[23]

3.49 The Committee takes the view that ambiguity in the application of this kind of legislation has the potential – however unintentional – to give rise to use of powers which would be proscribed under one statute but permitted under another, as in the example given by EFA. Accordingly, the Committee makes the following recommendation:

Recommendation 3

3.50 The Committee recommends that the bill and the TI Act be amended to ensure that the circumstances in which similar kinds of surveillance devices are authorised, are clearly described, and that the limitations on their respective use are also clear.

Accountability for outcomes

3.51 The Bill requires the keeping of records of the results of the warrant, including whether or not it was executed, and if so, what the outcome was. The chief officer of a law enforcement agency is required to keep a comprehensive register of the warrants applied for. This applies to all warrants and authorisations.

3.52 The Minister must receive a report as well as a copy of the warrant and associated documents. The agency must also provide an annual report to the Minister which includes an account of the outcomes in matters where the warrants were sought.

3.53 The Committee contrasts this provision with the requirement in some jurisdictions (for example in NSW under the *Search Warrants Act 1985*) for the applicant to provide a report after executing the warrant to the issuing officer. As

---

23 *Committee Hansard*, 10 May 2004 p. 10

noted, in this bill Clause 49 requires the CEO of an agency to report to the Minister, and include with a copy of the warrant, the information under subclause 49(2). There is no requirement to involve the issuing judge or member in the reporting process, which could also have implications for the exercise of the determining authorities' powers in granting either extensions or revoking the warrant.

3.54 The Attorney General's Department was asked why the report is not provided to the judicial officer who issued the warrant. The Committee was advised:

> That is something that does not exist in any Commonwealth legislation. The idea of reporting back to the judge who issued the warrant comes from Victorian legislation. … The advice that we had from Victoria was that their reports are in writing and are filed with the court documents. This did not really seem like a terribly successful oversight regime to us, so we discussed it with the AAT. The AAT said they did not wish to have these records that required secure storage and so on. Reporting to the minister and the Parliament seemed a much more satisfactory regime and it was more consistent with similar regimes in Commonwealth legislation.[24]

3.55 The Committee also notes that where records are required to be kept they may be inspected by the Ombudsman. The Committee accepts that this is a sufficient level of accountability.

Security of the information obtained

3.56 The provisions in Part 6 of the bill restrict quite heavily the use, communication and publication of information obtained from a surveillance device under a warrant, and from a device where a warrant was not obtained and should have been. There are significant custodial penalties for offences.

3.57 The protection extends to:

> 44(1) (c) any information that is likely to enable the identification of a person, object or premises specified in a warrant, an emergency authorisation or a tracking device authorisation.

3.58 Clearly the personal identification is protected in most circumstances and the issue is further clarified in section 45, which prescribes penalties for using, recording communicating or publishing protected information, and using it where it endangers the health or safety of a person or prejudices the effective conduct of an investigation into a relevant offence.

3.59 Mr Patrick Emerton from Monash University Law School was concerned at the 'sweeping provisions' contained in sections 44 and 45:

---

24 *Committee Hansard* 10 May 2004 p. 51

> They do not simply oblige police officers to protect the integrity of investigations they are engage in. They seem to prohibit any discussion, whether by suspects, journalists or any members of the public, of the details of any surveillance activities by the police. The offence created under subsection 45 (2) seems particularly extreme, as there is no requirement that the offender have any intention to obstruct justice or an investigation in communicating the prohibited information.[25]

3.60 While the Committee notes Mr Emerton's concerns, the section refers to protected information which is defined in subclause 44(1) as:

- information obtained under an authorised device;or
- information about a warrant including applications for emergency approvals;or
- information identifying a person or premises specified under a warrant; or
- unauthorised information obtained under a warrant.

3.61 The offence under subclause 45(2) is for communicating, recording or publishing protected information, not authorised by the section and endangering the health or safety of a person. There are exceptions to this prohibition provided in subclause 45 (4). They include:

- the use of material lawfully disclosed in court;or
- the use by a person to help prevent or reduce the risk of serious violence to a person or damage to property;or
- communication with the Director- General of ASIO or an officer of ASIO relating to the functions of the organisation; or
- communication with an agency head or a staff member within the meaning of the *Intelligence Services Act 2001; or*
- In communication – under certain circumstances – with a foreign country.

3.62 Mr Emerton's concerns illustrate the difficulties in achieving a balance between protection of privacy, law enforcement and limitations on use of the information. These particular provisions are similar to those contained in the Model Bill developed by the Standing Committee of Attorneys General and the Australian Police Ministers Council Working Party referred to above, which in turn draws on provisions in the Customs Act, the TI Act and State and Territory legislation.[26] The sensitivity of the information which could be obtained – including matters of national security – leads the Committee to conclude that the provisions are appropriate in the circumstances.

---

25 *Submission* no 1, p.4

26 Cross Border Investigative Powers for Law Enforcement: Discussion Paper, p. 301-303

Remedies for breach

3.63 The Committee notes that there are no civil remedies for unlawful use of a surveillance device. This contrasts with the TI Act in which there is a regime for persons who are aggrieved by actions under the Act.

3.64 When asked about these civil remedies, the NSW Council for Civil Liberties explained:

> We think that people should be able to launch such action and, indeed, going through the legislation I could not see that there was any provision for that. I would have thought that if it were not addressed it would not take away a person's right to sue civilly but, as you will know, under Australian law there is no definite right to privacy. … I think it would be better if it were made clear in the bill that in the case of abuse there is a civil right for people who have been damaged by breach of these conditions.[27]

3.65 The Committee notes that even if the right to sue civilly, is available, it is likely to be a more expensive and circuitous route to compensation for a breach of the Act than a right given under the Statute.

3.66 In response, the ACC pointed to administrative procedures for compensation available, plus the option of a complaint to the Ombudsman.[28]

3.67 The Committee also heard that there could be complications with adding provisions for civil remedies for breach. As officers of the Attorney General's Department told the Inquiry:

> It is partly because of the complexity of the match between Commonwealth and state laws here. Given that we have no power directly over surveillance devices, we have not made the use of any of these devices unlawful. We are totally reliant, as Mr Batch told the committee, on state laws to prohibit the use of them. Therefore, while we provide a regime that authorises law enforcement use, the fact that it falls outside that regime, particularly as to the optical surveillance device area, does not mean that it is necessarily unlawful. [29]

3.68 The Committee remains concerned that there are no civil rights to compensation under the proposed legislation. While appreciating the complexity in relation to State legislation, the Committee does not accept that these problems are insurmountable and still considers the absence of such a right to be an anomaly.

Recommendation 4

---

27 *Committee Hansard,* 10 May 2004, p.16

28 *Committee Hansard*, 10 May 2004 pp 10–11

29 *Committee Hansard,* 10 May 2004, p.42

3.69 The Committee recommends that the bill be reviewed with the states in order to add civil remedies to the appropriate legislation for those who are affected by misuse of the devices.

A use-by date for information obtained?

3.70 The Committee observed that the comprehensive provisions concerning security of information do not apply equally comprehensively to the destruction of records. Under section 46, the chief executive officer of a law enforcement agency (or the officer in charge of an agency such as ASIO) is required to destroy (or cause to be destroyed) any record or report which contains protected information, subject to being satisfied that it is not likely to be required in connection with a purpose described in sections 44 or 45. These sections broadly described the circumstances under which protected information may be used, such as in investigating a relevant offence (of which there are seven).

3.71 The Committee considers that despite the protected nature of the information, there should be some specific point at which the material must be destroyed. A time limit of five years could be set, with a provision which allows an agency still requiring the material for investigation or court purposes, to justify its retention.

3.72 The independent oversight of the destruction of the records was also raised by the Committee. While the Ombudsman is required to inspect the agency's records, including the decision-making process,[30] there is no requirement for the Ombudsman or his delegate to be present at the destruction of records.

3.73 In relation to the independent oversight of the destruction of records, the Attorney General's Department told the hearing:

> … we require the agency to keep a record of the destruction and for that to be available to the Ombudsman. I do not know how feasible it would be to have somebody physically present when these records are destroyed. I would imagine that there will be a very significant number of these that are destroyed on a more or less continuous basis. I do not think that you could batch them up and then destroy them every three months or so. That really would not be consistent with the philosophy of the legislation of destroying them when you decide that they are no longer relevant.[31]

3.74 The Department provided further information from the Senior Assistant Ombudsman who said:

> In my view the mere attendance of an Ombudsman staff member when the material is destroyed would not provide any additional degree of accountability concerning the destruction process. In order to provide such a level of assurance, Ombudsman staff would need to exercise

30 Submission 7, p. 3

31 *Committee Hansard,* 10 May 2004, p.52

> comprehensive oversight in relation to the whole process, from the point of the records' creation to their destruction. This regime would necessarily entail a significant amount of 'real time' monitoring within the agencies and would not be feasible with existing resources.
>
> In our view, it would be more desirable if the Ombudsman's accountability role in relation to destruction of SD material were consistent with his role in relation to TI material. This role would enable retrospective procedural inspection of the destruction process (such as the identification, approval and destruction of SD material) without being present when the material is destroyed.[32]

3.75 The Committee also accepts that requiring a process to justify the non-destruction of records, or have the destruction witnessed by an officer from the Ombudsman's office would have significant resource implications for all agencies concerned.

3.76 The Committee's principal concern is that there be a statutory limit on the length of time that material derived from surveillance devices may be kept, with the power to extend that time under stated circumstances to reside with the CEO of the agency concerned.

3.77 The Committee accepts the suggestion by the Senior Assistant Ombudsman that the destruction provisions in this bill be brought into line with the TI legislation.

32 *Submission* no 8, p.3

Recommendation 5

3.78 The Committee recommends that the legislation be amended to include a time limit for retention of material of five years, subject to the agency being required to provide justification – certified by the CEO – as to why the material is still needed.

Recommendation 6

3.79 The Committee also recommends that the destruction provisions in this bill concerning records kept be brought into line with the provisions contained in the TI legislation.

Differences between this and other similar legislation.

3.80 As is evident from the foregoing discussion, the Surveillance Devices Bill is inconsistent with the provisions of other Commonwealth legislation – particularly the TI Act – notwithstanding their closely related subject matter. The Attorney General's Department explained that these differences arise because the bill 'is modelled largely on the joint working group model rather than specifically on the telephone intercept legislation'.[33]

3.81 Also relevant is the fact that the TI legislation was written in 1979 and the operating and technological environment has changed considerably in that time. For example, in 1979 telephones operated only on land lines which had very specific technology attached to interception. That technology is irrelevant for mobile phones, which operate in a completely different technological environment. The TI Act has also been amended from time to time to reflect these changes.

3.82 In relation to the apparent inconsistencies with other legislation, the ACC also said:

> Perhaps some of the differences result from the different origins. For example, the Surveillance Devices Act was not really written from the ground up by the Commonwealth; it was partly adopted from a model developed by a joint working group and then, in a sense, modified to fit in with the Commonwealth legislative scheme. It reflects some of the provisions of the TI Act. So there would be those minor differences.[34]

3.83 The Committee appreciates that the legislation was developed with State considerations in mind and that it probably suffers from the need to accommodate in its requirements a number of operational environments. However, as a general principle, the Committee considers that to the extent possible, the Commonwealth legislative regimes that deal with surveillance activities by law enforcement agencies

---

33 *Committee Hansard*, 10 May 2004, p.34

34 *Committee Hansard,* 10 May 2004, p.5

should be consistent in relation to matters such as the granting of warrants, time limits, accountability and remedies for breach.

3.84 Notwithstanding the differences in the methods of surveillance, the lack of an overarching regime applying to search warrants, surveillance devices or TI devices is confusing may result in misuse by some law enforcement officers. In contrast, a more uniform system provides a reliable and predictable operating environment for surveillance professionals and more consistent protection of privacy.

Conclusion

3.85 The Committee welcomes the introduction of legislation to regulate surveillance devices. However the Committee concludes that the bill could be improved by amendments to provisions concerning emergency applications, the provision of records for optical surveillance devices, the availability of civil remedies, and the use of similar devices under the proposal and the TI Act.

Recommendation 7

3.86 The Committee recommends that the bill be passed, subject to the recommendations set out above.

Senator Marise Payne
Committee Chair

APPENDIX 1

Submissions Received

1	Monash University
2	Australian Crime Commission
3	New South Wales for Civil Liberties
4	Office of the Victorian Privacy Commissioner
5	Australian Federal Police
5A	Australian Federal Police
6	Law Council of Australia
7	Attorney – General's Department
8	Electronic Frontiers Australia Inc.

APPENDIX 2

Witnesses who appeared before the Committee at public hearings

Canberra, Monday 10 May 2004

Australian Crime Commission

Mr Brian Dargan, Manager Law Reform and Commercial Legal

Mr Robert Tebbet, National Manager, Technical and Physical Surveillance

Mr Raymond Tinker, Head of Investigation South East Asia Organised Crime

New South Wales Council for Civil Liberties

Mr David Bernie, Vice President

Office of the Victorian Privacy Commissioner

Mr Paul Chadwick, Privacy Commissioner

Ms Michelle Fisher, Manager, Policy

Australian Federal Police

Mr John Lawler, Performing the Duties of Deputy Commissioner

Mr David Batch, Senior Legislation Officer

Mr Rudi Lammers, Manager Technical Operations

Attorney General's Department

Ms Maggie Jackson, Special Adviser, Criminal Justice and Security Group

Mr Nick Smith, Senior Legal Officer, Security Law Branch