



REPORT OF THE REVIEW OF THE REGULATION OF
ACCESS TO COMMUNICATIONS

ANTHONY S BLUNN AO

AUGUST 2005

© Commonwealth of Australia 2005

ISBN: 0 642 21158 2

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>

Produced by Public Affairs Unit,
Australian Government Attorney-General's Department
Publication number

Table of Contents

Review of the Regulation of Access to Communications	1
<i>Terms of Reference</i>	3
<i>Findings</i>	5
<i>Recommendations</i>	10
1. From Interception to Data Access – the Shift	14
1.1. <i>General Observations</i>	14
1.2. <i>The Current Access Regime</i>	21
1.3. <i>From Interception to Data Access</i>	24
1.4. <i>Access in ‘Real Time’ – Interception</i>	26
1.5. <i>Stored Communications</i>	28
1.6. <i>Access to Stored Data – The Basic Concepts</i>	32
1.7. <i>Access to Call Data</i>	34
1.8. <i>Stored Communications – The Critical Interface</i>	36
2. Interception Capability Compliance	39
3. Technology – The Developing Challenges	44
3.1. <i>Introduction</i>	44
3.2. <i>Problems of Identification</i>	45
3.3. <i>The Problems of Data Capture and Understanding</i>	47
4. Cost Implications	49
5. The Protection of Information Systems	52
6. The Classification of Offences	54
7. Protective Access	57
8. The Reporting Structure	63
9. The Use and Destruction of Data	69

10. Data Access for Intelligence Purposes	71
11. Other Emerging Technologies	73
12. B-Party Interceptions	75
ATTACHMENT 1 – SUBMISSIONS RECEIVED	78
ATTACHMENT 2 – REQUIREMENTS FOR CLASS 1 AND CLASS 2 OFFENCES	79
ATTACHMENT 3 – LAW ENFORCEMENT REPORTING STRUCTURE	82

Common Terms and Abbreviations

ACA	Australian Communications Authority
ACMA	Australian Communications and Media Authority
ACC	Australian Crime Commission
ACS	Australian Customs Service
AFP	Australian Federal Police
AGD	(Commonwealth) Attorney-General's Department
Agency Co-ordinator	As defined in section 7 of <i>Telecommunications Act 1997</i>
ASIO	Australian Security Intelligence Organisation
CAD	Call Associated Data
CSP	Carriage Service Provider
C/CSP	carrier and carriage service provider
DCITA	Department of Communications Information Technology and the Arts
DPP	(Commonwealth) Director of Public Prosecutions
GSM	Global system for mobile communications
ICC	Interception Consultative Committee
ICP	Interception Capability Plan
IGIS	Inspector-General of Intelligence and Security
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Service Identifier
Interception Act	<i>Telecommunications (Interception) Act 1979</i>
IP	Internet Protocol
ISP	Internet Service Provider
LEAC	Law Enforcement Advisory Committee

MSISDN	Mobile Station International ISDN Number
NCSP	Nominated Carriage Service Provider
SIM	Subscriber Identity Module
SMS	Short Messaging Service
States	States and Territories
Telco Act	<i>Telecommunications Act 1997</i>
TI	Telecommunications Interception
TIRAC	Telecommunications Interception Remote Authority Connection
VoIP	Voice over Internet Protocol

Review of the Regulation of Access to Communications

Since 1994 there have been four major reports dealing with telecommunications interception.

They were:

- The 1994 review by Mr P. Barrett into the Long Term Cost Effectiveness of Telecommunications Interception;
- The 1999 review by Mr D. Boucher of Interception Arrangements under section 332R of the Telecommunications Act 1997;
- The 1999 review by Mr P. Ford of Telecommunications Interception Policy; and
- The 2003 review by Mr T. Sherman AO of Named Person Warrants and other matters.

I am indebted to those reviewers and many of the issues canvassed in my report find their antecedents in those reviews.

As part of my review I invited submissions from the public. That was done through an advertisement placed in the Canberra Times and The Australian newspapers on 2 April 2005. I also wrote to those parties which had demonstrated an interest in previous reviews and in the legislative processes related to the *Telecommunications (Interception) Act 1979*. As a result I received some 31 submissions. A small number of those submissions were classified and are therefore not identified in the listing of submissions at Attachment 1. I also met with a number of individuals and organisations including the major carriers, security and law enforcement agencies and with privacy interests, to elaborate issues where I felt that was necessary. I am grateful to all those who have contributed.

I should also acknowledge my particular gratitude and indebtedness to Ms Catherine Smith and Ms Raewyn Miners of the Attorney-General's Department for their unstinting assistance and very willing cooperation. There are of course many other officers both of the Attorney-General's Department and the Department of Communications Information Technology and the Arts that will recognise in the report the contribution they made. I am grateful to all of them.

It is inevitable that there will be further reviews. Indeed given the rate of changes within the industry and within society more generally I believe that there is a strong case for regular reviews, say at three yearly intervals. The complexity and significance of the issues makes it problematic for unversed persons to do justice to them within a reasonable time frame. I am not a fan of committees but there may be advantage in there being a standing representative committee structure which could do or at least provide support for future reviews.

Anthony S Blunn AO
Canberra
August 2005

Terms of Reference

I am asked to:

‘review the policy options for the regulation of access to telecommunications with particular emphasis on new and emerging telecommunications technologies’

having particular regard to:

‘protecting the privacy of users of the system;

‘the assistance that accessing the content of telecommunications offers in

- investigating serious crime and threats to security, and
- providing certainty to agencies seeking access and for users of the system’,

and to consider and comment on:

‘the ongoing appropriateness of the current telecommunications interception regime and (if relevant) alternatives for the lawful access to content;

‘the protection of information systems from attack by means of the telecommunications system, including the use of intrusion detection systems and other measures;

‘the cost implications, including cost recovery mechanisms; and

‘such other issues as they arise out of the review’.

In the course of the review I have had regard to the views of the Legal and Constitutional Committee of the Senate in its Report on the Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004, that the review should:

- examine the issue of whether an internet service provider (ISP) can identify whether a message has been accessed by the intended recipient;

- consider whether a review of the content of ongoing and outgoing e-mails for IT and other screening purposes could be achieved by amending the Act to provide for specific exemptions;
- consider whether the existing legislative obligations in relation to the destruction of unnecessary or irrelevant information (i.e. that is not needed in an investigation) are adequate;
- consider what accountability mechanisms apply when agencies and other parties use some form of ‘lawful authority’ to access stored communications and whether they are adequate to protect the privacy of those using short messaging systems (SMS); and
- reconsider the appropriateness of continuing the exemption of read and unread stored communications from the telecommunications interception regime as proposed by [the] Bill.

Findings

That, as identified in the body of my report:

- the protection of privacy should continue to be a fundamental consideration in, and the starting point for, any legislation providing access to telecommunications for security and law enforcement purposes;
- access to telecommunications data is, and for the foreseeable future will remain, fundamental to effective security and law enforcement;
- new and emerging technologies provide unprecedented levels of security for users and make access for security and law enforcement purposes more problematic;
- those technologies will require security and law enforcement to make more use of, and as appropriate develop, alternative techniques, including other perhaps more intrusive, forms of electronic surveillance to compensate for any loss of access to telecommunications data;
- the basic concepts and structures of the *Telecommunications (Interception) Act 1979* which provide for access in real time (i.e. interception) to telecommunications reflect an appropriate balance between protecting privacy and meeting the needs for access by security and law enforcement agencies;
- there are good reasons for distinguishing between intercepting real time communications and accessing ‘stored’ data;
- all real time access to data that contains content should continue to be subject to an interception warrant;
- the language and detail of the *Telecommunications (Interception) Act 1979* are increasingly limiting in terms of accommodating new and emerging technologies, in

terms of industry development and in terms of responding to the needs of security and law enforcement agencies;

- there is a need for a system of user and/or equipment identification that is unique, indelible and available;
- the present distribution of functions relating to accessing telecommunications data for security and law enforcement purposes between Parts 13, 14 and 15 of the *Telecommunications Act 1997* and the *Telecommunications (Interception) Act 1979* is complicated, confusing and dysfunctional;
- as presently structured, the *Telecommunications (Interception) Act 1979* is not an appropriate vehicle for accessing other than real time communications;
- the provisions of the *Telecommunications Act 1997* governing access to stored communications are inadequate and inappropriate;
- for interceptions to remain effective it is essential that the capacity to intercept communications traffic continue to be provided by carriers/carriage service providers and that product be provided in useable form and where other services are involved including value added services, the service provider be required to provide the product in useable form;
- the current regime to access call associated data should be maintained but the requirement for data to be released only on the authority of a conforming certificate should be reinforced;
- the provisions of subsections 282(1) and (2) of the *Telecommunications Act 1997* should be reviewed to better identify their scope and make clearer their operation;

- there is a need for legislation which deals comprehensively and over-ridingly with access to telecommunications of all forms of communications data for security and law enforcement purposes;
- information systems, as part of the critical national infrastructure, are currently appropriately protected in terms of the assessed risk but there is no room for complacency, particularly in the area of personnel security;
- the current models for the distribution of costs between the industry and security and law enforcement are appropriate in relation to traditional telephony;
- in relation to Internet Protocol (IP) and other communication networks the principle should be that carriers/carriage service providers meet the cost of providing access to data travelling over a specified connection and that the provider of any other services including value added services travelling over that connection should be required to meet the costs of providing communications in useable form;
- carriers/carriage service providers should be entitled to recover their reasonable costs on the basis of the no loss/no gain formula whenever and to whomsoever they provide data;
- whilst operational funding appears generally satisfactory the resourcing of support functions essential to the data access regime at least at the Commonwealth level is inadequate and unless remedied will increasingly impact on operational effectiveness;
- increasingly the development and application of new technologies are determined internationally;

- it is critically important that Australia at least maintain and preferably increase its involvement in international fora in which the requirements for access by security and law enforcement agencies are identified and agreed;
- there is a need for greater emphasis on communication and stakeholder education about the issues facing data access for security and law enforcement purposes;
- the tasks of maintaining the registers which form the basis for the reports to the Minister and the general oversight of warrants currently performed by the Commissioner of the Australian Federal Police could be more effectively done by the Office of the Agency Co-ordinator;
- it is difficult to see any useful purpose served by the current requirements for State Ministers to provide the Attorney-General with copies of warrants, revocations and reports;
- the requirement for the Commissioner of the Australian Federal Police to be informed of and provided with copies of all law enforcement warrants and revocations is neither necessary nor appropriate;
- there is an argument for permitting law enforcement agencies subject to stringent controls to retain some accessed communications data for ‘intelligence’ purposes;
- there is an argument for permitting selected law enforcement agencies subject to stringent controls to access communications for the purposes of obtaining intelligence for law enforcement purposes;
- there is a need to consider the implications of wireless technology in terms of access for security and law enforcement purposes with particular emphasis on the need to maintain access where communications transfer from system to system;

- the effectiveness and efficiency of the current interception regime depends significantly on the power to grant exemptions;
- the current scheme in relation to exemptions whilst workable, is a confusion of responsibilities and accountabilities between Ministers and Departments and Agencies;
- there is a need for a more effective compliance regime but responsibility should remain with the Australian Communications and Media Authority as the industry regulator;
- the distinction between Class 1 and Class 2 offences produces no meaningful difference in terms of outcomes;
- there would be advantages were Class 1 and Class 2 offences to be identified simply by reference to prescribed periods of imprisonment;
- there are circumstances in connection with the protection of data systems or with the development and or testing of new technologies where the incidental interception of communications should be permitted subject to appropriate controls.

Recommendations

I recommend that:

- i. comprehensive and over-riding legislation dealing with access to telecommunications data for security and law enforcement purposes be established;
- ii. the basic elements of the *Telecommunications (Interception) Act 1979* relating to privacy and to access to real time communications should be incorporated into and form the basis of any such legislation which should also incorporate the relevant parts of the *Telecommunications Act 1997*, principally elements of Parts 13, 14 and 15;
- iii. Australia at least maintain and if possible increase its involvement in those international fora concerned with or related to access to communications for security and law enforcement purposes and that appropriate resources for this purpose be provided on an assured basis;
- iv. in the absence of universally accepted international standards, binding Australian standards for interception capability be developed which incorporate any appropriate international standards or guidelines;
- v. the Office of the Agency Co-ordinator be given the responsibility for providing legal advice on the relevant access legislation, at least in so far as Commonwealth agencies are involved;
- vi. the Office of the Agency Co-ordinator give greater emphasis to communication with and education of stakeholders and that appropriate resources be made available for that purpose;

- vii. access to telecommunication data for surveillance purposes be reviewed in the context of considering the need for comprehensive and overriding legislation dealing with the general issue of access to telecommunications data;
- viii. in the context of accessing stored communications any specific reference to Voice over Internet Protocol (VoIP) is unnecessary and should be removed;
- ix. the distinction between real time access i.e. interception, and access to stored data be maintained;
- x. real time access to communications continue to be authorised by interception warrant;
- xi. access to stored communications continue to be authorised by search warrant but those warrants be required to meet minimum prescribed standards;
- xii. except as otherwise prescribed call data continue to be accessed only on the authority of a conforming certificate;
- xiii. having regard to the privacy implications the provisions of subsections 282(1) and (2) of the *Telecommunications Act 1997* be reviewed with a view to clarifying their intent and scope and better identifying the processes to be followed;
- xiv. the provisions of the *Telecommunications Act 1997* and the *Telecommunications (Interception) Act 1979* regarding the responsibilities and accountabilities of Ministers, Departments and agencies in relation to the requirement to lodge interception capability plans and the exemption processes in relation to those plans be rationalised to focus on the role of the Agency Co-ordinator;
- xv. responsibility for industry compliance with interception obligations should remain with the Australian Communications and Media Authority but an effective

compliance scheme should be developed in consultation with the Agency
Co-ordinator and implemented;

- xvi. as a matter of priority a unique and indelible identifier of the source of telecommunications be developed as the basis for access;
- xvii. carriers/carriage service providers be required to impose on service providers for whom they carry data, the obligation to interpret that data or at least the means to decode it in order to provide useable data to security and law enforcement agencies;
- xviii. in relation to traditional telephony the current model for the distribution of the costs of access between carriers/carriage service providers and agencies be maintained;
- xix. in relation to Internet Protocol (IP) and other communication networks, carriers/carriage service providers should meet the costs of accessing data travelling over a specified connection and that the provider of any other services including value added services travelling over that connection should be required to meet the costs associated with providing communications to the agencies in useable form;
- xx. carriers/carriage service providers be authorised to recover their reasonable costs of providing information on the basis of the no loss/no gain formula regardless of the form of the request or order;
- xxi. the security of information systems as part of the critical national infrastructure, be regularly assessed and that personnel security be given particular attention;
- xxii. the distinction between Class 1 and Class 2 offences should be removed;
- xxiii. Class 1 and Class 2 offences should be identified solely by reference to the prescribed period of imprisonment;

- xxiv. subject to appropriate controls access to communication without warrant should be permitted where it is necessarily incidental to the protection of data systems or the authorised development and or testing of new technologies;
- xxv. the requirement for the Commissioner of the Australian Federal Police to be provided with and to review and authorise the implementation of all law enforcement interception warrants be abolished;
- xxvi. the Office of the Agency Co-ordinator be made responsible for maintaining those registers required in relation to the Attorney-General's obligations to review the use of interception powers and that it be resourced appropriately for any additional functions involved in carrying out that role;
- xxvii. the views of State Ministers be sought on the value of requiring them to provide copies of warrants, revocations and reports to the Attorney-General and in the light of those views the requirement be re-considered;
- xxviii. subject to appropriate controls, authorised law enforcement agencies be permitted to retain identified accessed data for intelligence purposes;
- xxix. subject to appropriate controls provision be made that allows authorised agencies to access communications content for the purpose of obtaining intelligence for law enforcement purposes;
- xxx. the impact of wireless technology be separately examined with a view to establishing an appropriate access regime having regard particularly to the interface between systems and the need to maintain continuity of access;
- xxxi. the appropriate legislation be amended to make it clear that B-Party communications may be intercepted in prescribed circumstances.

1. From Interception to Data Access – the Shift

1.1. General Observations

- 1.1.1. As reflected in the terms of reference the fundamental issue is the appropriate balance between the interests of privacy and those related to the protection of security and the maintenance of law and order.
- 1.1.2. However, increasingly the commercial importance of telecommunications requires that consideration be given to the competitive impacts of any controls over what is now a significantly deregulated telecommunications industry. Relatedly the critical role of telecommunications in maintaining, controlling and protecting the national infrastructure requires some re-consideration of those areas where access to communications is required for other than law enforcement or security purposes.
- 1.1.3. A general tenet has always been that communications intended to be private should be private. That general tenet is not peculiar to telecommunications but that form of communication has always been afforded a very high degree of protection.
- 1.1.4. That protection is established by a combination of the *Telecommunications Act 1997* (the Telco Act) and the *Telecommunications (Interception) Act 1979* (the Interception Act). Whilst both Acts are important in regulating access to telecommunications it is the Interception Act which establishes a national scheme for the lawful interception of telecommunications by security and law enforcement agencies.
- 1.1.5. In large part because it is ‘technologically neutral’ the Interception Act has proved remarkably robust in an age of revolutionary technological change. However,

communication techniques globally, are going through dramatic, interrelated and continuing changes both in relation to the nature and application of technology and in terms of the social and commercial environment in which they operate.

- 1.1.6. The technology and its ready availability of that technology now provide very significant privacy protections. That technology and the consequential manner, volume and speed of communications also create new problems for security and law enforcement agencies in accessing those communications.
- 1.1.7. Threats to security and law and order are real, they are insidious, often international in scope and difficult to counter. The interception of voice communication, has been, and still is, amongst the most effective methods of obtaining evidence and intelligence. It is not infrequently the only method. In a number of situations it is almost certainly the most cost effective.
- 1.1.8. Cost and other resource constraints are already resulting in increasingly selective targeting of interceptions. This trend will almost certainly continue.
- 1.1.9. Interception of voice communication whilst of critical importance is only one aspect of data access. Increasingly telecommunications are in the form of data transfers which are capable of being intercepted while they are passing over the network but may also be stored. There is a need therefore to consider both real time access, i.e. interception and access to so called stored communications.
- 1.1.10. **For the reasons outlined in subsequent parts of this report it is my view that the current legislative framework is inadequate and that there is a need for comprehensive and over-riding legislation dealing with access to telecommunications for the purposes of security and law enforcement and I recommend that such legislation be established.**

- 1.1.11. **The basic elements of the *Telecommunications (Interception) Act 1979* relating to privacy and access to the content of real-time communications are in my view appropriate and effective and I recommend that they be incorporated into and form the basis of any such legislation which as subsequently elaborated should also incorporate the relevant parts of the *Telecommunications Act 1979*.**
- 1.1.12. Whilst emerging technologies are a growing and very real challenge to currently used interception techniques, alternative techniques are being and will continue to be developed which will challenge the existing legal framework. Encryption, long identified as an emerging problem for interception, is becoming increasingly available on standard products, it is simple to use and relatively inexpensive and as a consequence its uptake is finally becoming a real issue. Emerging wireless technology poses new challenges. Though responses to those and other technologies are unlikely to provide the same utility they will almost certainly involve significantly higher costs for security and law enforcement agencies and will be more operationally complex.
- 1.1.13. Increasingly the development and application of new communication technologies are determined outside Australia. Taking advantage of those technologies is critical to Australia's competitive position across a wide range of interests. That dependence does create some problems for achieving an effective regime for data access. However they are not insuperable. At least most developed nations including the technology developers have similar requirements for data access. Whilst the use made of data may vary across legal systems the common need for access will continue to influence development. International concerns about security and law enforcement can only increase that influence.

- 1.1.14. **Accordingly I recommend that Australia maintain and even increase its involvement in international fora in which the requirement for access for security and law enforcement purposes are identified and agreed and that appropriate resources be provided to make this possible on an assured basis.**
- 1.1.15. Relatedly, because most of Australia's telecommunications equipment is designed and manufactured overseas, and because of the need for compatibility, it is inevitable that Australia must adopt international standards. This is reflected in the requirement that any Determination made by the Attorney-General in relation to interception capability or special assistance capability must specify an international standard or guideline on which the Determination is based (section 322 of the Telco Act). To date the Attorney-General has not made any Determination under section 322. To the best of my knowledge this has not caused any major problems but the increasing requirements in relation to access capability are likely to create a demand for such a Determination. At issue is that there is no universally accepted international standard or guideline. Whilst the Attorney-General is only required to identify 'an international standard', given the underlying reasons for the requirement, the intent is that the identified standard be relevant to Australia's supply situation and network compatibilities.
- 1.1.16. It is relevant that the Determination must adopt, apply or incorporate the whole or a part of the international standard with only such modifications as are necessary for its application in Australia. In short, the provision seems at the same time to be both too prescriptive and too vague.
- 1.1.17. As with much of the data access regime, effectiveness is dependent on shared understandings of what is required and what is practicable. Whilst I have no doubt that there would be consultation with the industry prior to any

Determination being made it would appear appropriate were it to be made a requirement. **For the reasons outlined, whilst in my view any Determination should reflect, and not be inconsistent with, an appropriate international standard it would seem sensible in the interests of certainty for the Attorney-General to have a wider power to make Determinations in relation to interception capabilities particularly where there is no appropriate international standard and I recommend accordingly.**

- 1.1.18. The need for shared understandings highlights the requirement for a greater emphasis on communication and education on issues facing data access for security and law enforcement purposes. In my view there is a pressing need to ensure that all involved in giving effect to the data access regime are kept better informed of current legal and related issues and developments. Obviously this would include carriers/carriage service providers (C/CSPs) but would extend to vendors and to privacy interests. It might also sensibly involve the Director of Public Prosecutions (DPP) and the issuing authorities provided any suggestion of influence could be avoided.
- 1.1.19. The Interception Consultative Committee (ICC), which is chaired by the Agency Co-ordinator, already provides an effective mechanism for consultation between the Attorney-General's Department (AGD) and the intercepting agencies. The Law Enforcement Advisory Committee (LEAC) already provides a useful contact forum for industry and security and law enforcement agencies but in my view could be better focussed on the structured resolution of issues rather than simply talking about them.
- 1.1.20. There is support in the agencies for a major forum that brings together the wider population of parties involved with telecommunications access for law

enforcement and security purposes. Indeed I am informed that one such annual forum did exist until relatively recently and it is generally regarded as having performed a valuable role that is no longer met. The reason for the demise of the forum is ascribed to a lack of clear understanding about responsibility for funding which led to a unilateral decision to change the established relationship which was regarded by most participants as unfair. Whilst the re-establishment of such a conference would be one way to meet the need for better information sharing there may well be others such as the greater use of video forums etc. In my view there is a need – what is required is a mechanism and clear understandings about responsibilities and cost attribution. As the need is related to achieving basic Commonwealth objectives the Commonwealth should be prepared to accept the major funding and organisational responsibilities.

1.1.21. However in my opinion what is required even more is a sustained program of contacts designed both to inform and learn and involving those essential to maintaining the effectiveness of the access regime. Such a programme may reduce the uncertainties which result in the confusion of often conflicting opinions about the interpretation of the Interception Act. **In this context at least in relation to Commonwealth agencies it may be desirable for the provision of advice to be focussed in the Office of the Agency Co-ordinator. I recommend that this be done.**

1.1.22. The Office of the Agency Co-ordinator is a statutory office established by the Telco Act and is the central point of contact for intercepting agencies and industry on telecommunications interception issues. Its functions include seeking the views of the intercepting agencies on interception capability issues and providing legal and policy advice on aspects of the Telco Act and the Interception Act.

- 1.1.23. The Office of the Agency Co-ordinator in the Attorney-General's Department would appear to be best equipped to manage such a communication education program although obviously to be effective it would need to involve representatives from a number of agencies.
- 1.1.24. **Accordingly I recommend that the Attorney-General's Department give greater emphasis to communication with, and education of, stakeholders and that appropriate additional resources be made available for that purpose.**
- 1.1.25. An issue which arose during the review was the use of telecommunications data for surveillance purposes. Mobile telephones provide locational data and the precision of that data can be expected to improve. That data is generated without any specific intervention. The use of that data for security and law enforcement purposes is obvious. The privacy implications are equally obvious. However it is far from clear whether access is subject to any regulation. What does seem clear is that the issue is about access to telecommunications data.
- 1.1.26. **Accordingly I recommend that the access to such data for surveillance purposes be considered in the context of the requirement for comprehensive and over-riding legislation dealing with the general issue of access to telecommunications data.**

1.2. The Current Access Regime

1.2.1. As previously identified access to telecommunications is regulated through the provisions of the Telco Act and the Interception Act.

The Telecommunications Act

1.2.2. Very broadly the Telco Act, in so far as it is relevant, regulates the networks that carry, or are capable of carrying, communications by means of guided or unguided electromagnetic energy. The scheme of the Act is built around a structure of licensed C/CSPs which constitute the network: relevantly it concentrates on the obligations of those C/CSPs and ‘associated persons’ in relation to accessing that network. Access is dealt with in Parts 13, 14 and 15 which respectively deal with:

- the protection of communications;
- national interest matters; and
- cooperation with agencies.

1.2.3. Importantly, Part 13 provides, amongst other things, that ‘eligible persons’ must not disclose or use any information accessed in the course of employment that relates to the content or substance of any communication that has been or is being carried by a C/CSP, the service supplied, or the affairs or personal particulars of another person. There are however, a number of exceptions, including, in relation to content or substance, where disclosure or use is required in connection with the operation of an enforcement agency under a warrant or in any other case is required or authorised by or under law. More broadly disclosure of information or a document, but not in relation to content or substance, is excepted where disclosure is certified by an authorised officer as reasonably necessary for the

purposes of national security, enforcing the criminal law or a law imposing a pecuniary penalty or protecting the public revenue.

1.2.4. Part 14 builds on Part 13 in requiring C/CSPs to do their best to prevent telecommunication networks and facilities being used to commit offences and to give authorities such help as is reasonably necessary for the purposes of:

- enforcing the criminal law and laws imposing penalties;
- protecting the public revenue; and
- safeguarding national security

and provides that they may, in an emergency, suspend a service if requested to do so by a senior police officer. Importantly, Part 14 identifies the terms and conditions, including the costing principles, on which help is to be given.

1.2.5. Part 15 provides the structures through which the obligations in relation to interception are imposed on C/CSPs. For those purposes interception consists of listening to or recording a communication in its passage over a controlled network or controlled facility.

The Interception Act

1.2.6. The Interception Act, other than by exception (e.g. stored communications), deals only with the interception of telecommunications ‘passing over’ a telecommunications system. Other than as provided the Act makes it an offence to intercept such communications.

1.2.7. For the purposes of the Act ‘interception’ consists of listening to or recording, by any means, a communication ‘passing over’ a telecommunication system without the knowledge of the person making the communication. ‘Passing over’ is not defined other than that it includes ‘being carried’ which itself is not defined

although ‘carry’ is defined to include ‘transmit, switch and receive’. Neither listening nor recording are defined, although ‘record’ in relation to interception is defined to include a record or copy of a communication in whole or in part whether in writing or otherwise made by means of the interception or obtained by the interception.

- 1.2.8. There are a number of exceptions to the prohibition against interception. For law enforcement purposes the most significant are those related to ‘stored communications’ and to interceptions ‘under a warrant’, although other exceptions are relevant to some specific issues canvassed later in this report and are dealt with in that context. Information obtained under any one of the exceptions is ‘lawfully obtained information’. The Commonwealth Act then establishes an elaborate regime for authorising interception warrants. That regime admits State and Territory authorities where the Minister (the Attorney-General) is satisfied that the law of that State or Territory meets the prescribed conditions which impose accountability and reporting requirements related to the protection of privacy.
- 1.2.9. The Interception Act does not extend to services ‘carrying communications solely by means of radiocommunication’. I comment on this aspect later in this report.

1.3. From Interception to Data Access

- 1.3.1. The Interception Act was originally structured around the need to control the real time interception of telephony services which were then provided and controlled by the Commonwealth through the Postmaster-General's Department.
- 1.3.2. That basic structure is still evident in the current Act. As previously identified, because it is essentially 'technologically neutral' the Act has proved remarkably robust in the face of changing technology. The basic concepts relating to the protection of privacy; the effective control of interceptions through warrants issued in prescribed circumstances by independent and appropriately qualified persons; the requirements for effective control and ultimate destruction of intercepted material, and for tight oversighting and reporting regimes with identified responsibility to Ministers, have accommodated and are largely appropriate to the changes in technology.
- 1.3.3. However, the language and detail of the Act are increasingly being overtaken by the changes in technology and conditions. The definition of 'interception' by reference to 'listening to or recording' is itself an issue, although it has retained much of its utility through an interpretation of the word 'record'. However for greater certainly it would be appropriate for the definition to include 'read' given the development and significance of text messaging. The vexed issue of 'stored communications' arises in large part because of the requirement that in order to be intercepted, communications should be 'passing over' the system.
- 1.3.4. There are many such examples and the AGD is already actioning a number of proposed amendments to deal with specific problems. However, that process, whilst appropriate and necessary, is in my view unlikely to deal effectively with the underlying structural problems.

1.3.5. Amongst the most urgent of those is the need to satisfactorily resolve the tension between the idea of intercepting real time communications and accessing stored data.

1.4. Access in ‘Real Time’ – Interception

1.4.1. In my opinion, in terms of the basic concepts, access to real time communications is appropriately dealt with by the existing provisions of the Interception Act. Access to stored data is however not the subject of any comparable or effective legal regime designed to balance privacy interests with the need to maintain effective access to that data in the interests of security and law enforcement.

1.4.2. Although from a privacy point of view there may seem to be little difference, it seems to me that there are good reasons for distinguishing between intercepting real time communications and accessing ‘stored’ data. **Real time voice communications, including Voice over Internet Protocol (VoIP), which in my opinion and consistent with the objective of technical neutrality does not need to be and I recommend should not be separately identified, are likely to be more spontaneous than other forms of data communication and do not provide the opportunity for ‘second thoughts’ prior to transmission offered by those other forms.** As such, real-time access is akin to eavesdropping which was the comparison used by the then Attorney-General (Sir Garfield Barwick) when the Telephonic Communications Bill 1960 was introduced providing protection against unauthorised interception: viz,

‘eavesdropping is abhorrent to us as a people’.

Interception was then defined as ‘listening to or recording any communication in its passage over the telephone system’.

1.4.3. **Accordingly, I recommend that the distinction between intercepting real time communications and accessing ‘stored’ communications be maintained.**

- 1.4.4. Increasingly much of the data 'passing over' the telecommunication system are not voice communications. However it seems to me impractical and undesirable to suggest different regimes for real time access (i.e. interception) depending on whether the communication is voice or in some other form.
- 1.4.5. **Accordingly, I recommend that all real time access should continue to be subject to an interception warrant.**

1.5. Stored Communications

- 1.5.1. The Interception Act is now expressed to exclude ‘stored’ communications. The relevant amendment is ‘sunsetting’ and unless some action is taken before 15 December 2005, the provisions will lapse.
- 1.5.2. Currently access to the content or substance of communications stored within the system is achieved by general search warrant obtained under relevant Commonwealth or State Law which is executed under the provisions of the Telco Act, Part 13 of which prevents disclosure of content other than as prescribed.
- 1.5.3. That is consistent with, but in my opinion not necessarily a result of, the stored communications amendment of the Interception Act.
- 1.5.4. I am advised that there has been no increase in the number of complaints about access to communications since the passage of the ‘stored communications’ amendment.
- 1.5.5. Prior to the amendment it would appear that there were very different views about the application of the Interception Act to ‘stored’ communications. The issue turned on the interpretation to be given to the words ‘passing over the telecommunications system’ and therefore to the issue of at what point did a communication ‘commence’ and ‘cease’ ‘passing over’ the system and cease to be subject to the Act. In relation to when a communication ‘ceases’ passing over the system there are at least three competing views:
- (a) when the message has been received i.e. read by the intended recipient;
 - (b) when the message reaches the recipient’s receiving terminal; and

(c) when the message is 'stored' in the sense that it is at rest i.e. it is not being automatically processed by the telecommunications system and has reached the address from which it can be directly accessed by the intended recipient.

- 1.5.6. On all the evidence available, the first view is untenable. I am advised that with the new technology there is no reliable way for a C/CSP (or anyone else) to determine whether the intended recipient has accessed let alone 'read' a message.
- 1.5.7. The second view in effect requires that an interception warrant would be needed to access data at any point short of the intended recipient's personal terminal. In the main this would mean that, without an interception warrant, it would not be possible to access a message 'stored' by an Internet Service Provider (ISP). However it would be possible to access without an interception warrant communications that had not been 'sent' and those that had been 'received' i.e. were actually 'stored' in the recipient's computer, because they were not 'passing over the system'.
- 1.5.8. The third view broadly reflects the current situation. There are however some issues related to communications that are routed through equipment, say a firewall, installed to protect the system. This issue is discussed later in the report but for present purposes the issue can be categorised as one of stored communications.
- 1.5.9. It would appear that prior to the amendment to the Interception Act a number of agencies were acting on the understanding that the third view was even then the position at law and on that basis were accessing 'stored' communications other than by an interception warrant.

- 1.5.10. The amendment had the singular advantage of settling that issue at least for the time being. If the amendment lapses by the operation of the sunset clause nothing will have been settled and the previous unsatisfactory and uncertain position will be restored.
- 1.5.11. One way to avoid that result would be to further amend the Interpretation Act to define the concept of 'passing over' such that it included 'stored' communications.
- 1.5.12. In the view of most agencies if 'stored communications', irrespective of where they were 'stored', were to be made the subject of an interception warrant the consequences for law enforcement would be, in the words of the Australian Federal Police (AFP), catastrophic.
- 1.5.13. Under such a regime, the only way to obtain access, at least to the content or substance of stored communications, would be by interception warrant even where it was only suspected that stored communications might be relevant and by extension, and for the greater caution, in all cases because of the possibility that a telecommunications data storage device might be present. Such circumstances are unlikely to result in the issuing of a warrant. An obvious response might be to suggest that an interception warrant could be sought when the need for access to such a device was identified, say during a search under warrant. The equally obvious risk, in some cases at least, would be that any relevant data might not exist by the time an interception warrant was executed and in any event access can often be time critical.
- 1.5.14. Were such a regime to be adopted it would mean that many agencies which regularly use search warrants in the course of their operations, but which are not law enforcement agencies for the purposes of the Interception Act, e.g. the

Australian Customs Service (ACS), would be unable to access stored data.

Leaving to one side the question of whether some of those agencies, and ACS would appear to be one such, could sustain eligibility in terms of interception, it is likely that many which do not require real time access would not be approved as ‘intercepting’ agencies with consequent impacts for important aspects of law enforcement. Even for those that were approved the requirements of the Interception Act would almost certainly seriously limit their present capacity to carry out their statutory roles.

1.5.15. Assuming the current distinction between the interception of real time data and the access to stored data is accepted and access to stored data is not made subject to an interception warrant and, for the reasons outlined above, I believe that to be appropriate, it would still be necessary to distinguish between:

- (a) ‘stored’ data which, as identified above, discloses the content or substance of a communication; and
- (b) ‘call data’ which, although it varies with technology, is basically the ‘traffic information’ that records that a communication has occurred; (often) the time, duration and location of the ‘call’; and the addresses (numbers) of the sender and the intended recipient, in the internet environment this would be the IP address.

1.6. Access to Stored Data – The Basic Concepts

1.6.1. In terms of accessing the content or substance of communications data stored in the system, I recommend that the basic concepts of any scheme should I think be similar to those of the Interception Act namely:

- access to content or substance should only be by warrant;
- access to call data should only be provided on production of a certificate;
- warrants should meet identified minimum standards which should include that:
 - they should only be issued by an independent appropriately qualified authority e.g. magistrate or other person employed by a Court of a State or Territory who is authorised to issue search warrants;
 - they must clearly identify the suspected offence being investigated; and
 - they should specify that in the event of a telecommunications device being found it may be seized and or accessed for stored content;
- the warrant issuing authority should be required to have regard to the privacy implications of such a search and to the gravity of the matter under investigation in addition to any technical criteria that must be satisfied e.g. any maximum or minimum term of imprisonment that may be identified;
- it should be an offence to disclose any content data so accessed except as required by the processes of the investigation or any related investigation, and any subsequent prosecution, or for such other purposes as may be authorised by law e.g. secondary use; and
- any content data obtained should be securely stored and destroyed under supervision when no longer required for a permitted purpose.

- 1.6.2. Most law enforcement agencies have advised me that broadly they follow not dissimilar procedures now. That being so there should be little difficulty for them to accommodate such a regime. However, there are some agencies which have different requirements e.g. in relation to the issuing of warrants, and those agencies would need to meet the proposed minimum standards.
- 1.6.3. Access to the content or substance of communications ‘stored’ in electronic equipment in the possession (actual or constructive) of the intended recipient is not subject to the Telco Act. Currently access to such data is governed by a range of enactments both State and Commonwealth including the Commonwealth Crimes Act. However the privacy issues identified in relation to the data stored within the system seem to me to apply equally to stored data in the possession of the recipient and in my view the same data access procedures should apply.

1.7. Access to Call Data

- 1.7.1. As outlined at paragraph 1.2.3 currently under the Telco Act ‘call data’ may be accessed for security and law enforcement purposes and for the protection of public revenue. Generally the prescribed process involves an authorised officer of a designated agency certifying that disclosure is ‘reasonably necessary’ for the specified purpose. However under that process access to ‘content or substance’ is not to be disclosed.
- 1.7.2. **Other than to reinforce the requirement that access should only be provided on receipt of a conforming certificate I see no reason to change that regime and I recommend accordingly.**
- 1.7.3. However in what seems to me to be anomalous provisions, subsections 282(1) and (2) provide for the disclosure or use of information or a document, including content or substance, by an ‘eligible person’ (apparently to anyone) without any certificate, if the disclosure or use is reasonably necessary for the enforcement of the criminal law or laws imposing a pecuniary penalty or for the protection of the public revenue.
- 1.7.4. The provisions are intended to allow disclosure where an employee of a carrier in the course of employment comes across information which is clearly relevant to the enforcement of the criminal law but the information has not been requested by a law enforcement agency.
- 1.7.5. In as much as they require the eligible person to form an opinion that disclosure is ‘reasonably necessary’ for the enforcement of the criminal law or the protection of the public revenue they appear inappropriate and sit oddly with the requirement

established by subsections 282(3), (4) and (5) for a certificate from the requesting agency in which case access to content or substance is precluded.

- 1.7.6. That said, there is obviously a case for enabling eligible persons who do come across information in the course their employment which they consider relevant to security or law enforcement to report that to an appropriate authority. From a privacy point of view the provisions as presently drafted are not adequate and **I recommend that they be reviewed with a view to clarifying the objective and better identifying the process to be followed.** If they are to be retained, given the significance of the provisions, consideration should be given to them being incorporated in as a separate section.

1.8. Stored Communications – The Critical Interface

- 1.8.1. Currently access to stored communications and many other aspects related to access including interceptions for security and law enforcement purposes are governed by the provisions of Parts 13, 14 and 15 of the Telco Act. In my opinion those provisions, whilst workable from a security and law enforcement perspective, do not, from a privacy point of view, adequately reflect the basic concepts relating to either authorising the access to stored communications or to the storage and eventual disposal by agencies of accessed data.
- 1.8.2. In my view there is therefore a need to establish an appropriate legislative scheme which balances privacy considerations against the needs of security and law enforcement in terms of authorising access to stored communications and which at the same time provides greater certainty to the telecommunications industry.
- 1.8.3. I believe that will of necessity involve a review of Parts 13, 14 and 15 of the Telco Act.
- 1.8.4. As noted earlier the Telco Act regulates the providers of telecommunication services in Australia. As outlined below it imposes obligations on providers with regard to interception and provides the lawful basis on which agencies can seek assistance from industry.
- 1.8.5. Part 13 of the Telco Act provides protection and privacy to the content of communications, traffic data and personal information. It provides the basis for the disclosure of information by a C/CSP to ‘eligible persons’. In this regard the framework of the Part reflects the underlying premises of the Interception Act and like the Interception Act the Telco Act provides for access to private information in the course of a C/CSP’s business.

- 1.8.6. Part 14 deals with national interest matters including the obligations of C/CSPs to provide ‘reasonably necessary’ assistance to agencies, including in relation to the execution of warrants and the establishment of agreed delivery points.
- 1.8.7. Part 15 requires C/CSPs to cooperate with agencies including in relation to the provision of interception capability, the lodgement of interception capability plans (ICPs) and the allocation of costs. This last aspect is dealt with later in this report.
- 1.8.8. Importantly Part 15 identifies the role and legislative obligations of the Agency Co-ordinator. To my mind it is anomalous that the Agency Co-ordinator, an officer of AGD, is appointed by the Attorney-General under the provisions of an Act administered by the Minister for Communications, Information Technology and the Arts (Minister for Communications) to whom he is presumably accountable. This issue is dealt with in some more detail in considering the problems of data capture and understanding.
- 1.8.9. In my view, and as illustrated by the issue of stored communications, the provisions of these Parts which deal fundamentally with access to data for security and law enforcement purposes do not sit comfortably in the Telco Act. I am advised by officers of the Department of Communications, Information Technology and the Arts (DCITA) and AGD that the day-to-day administration of the provisions rests with the AGD and indeed I would be surprised were it to be otherwise.
- 1.8.10. Accordingly, at least in-so-far as they relate to accessing telecommunications data for security and law enforcement purposes, I have recommended that they be incorporated into legislation dealing comprehensively and over-ridingly with data access. This would provide a basis for consistency in application, greater responsiveness and remove the confusion caused by different legislation

providing different regimes and using different language for what are basically the same issues.

- 1.8.11. It is however in my view essential to maintain the involvement of the Australian Communications and Media Authority (ACMA) and other elements of the Communications portfolio as the industry regulators. It would for example seem appropriate to retain in the Telco Act those provisions which relate to the general controls over disclosure other than in relation to security and law enforcement.
- 1.8.12. Even in relation to security and law enforcement the Communications Portfolio would represent the interests of the industry but in my view that role should not be decisive. In the event of a conflict between the interests of security and law enforcement on the one hand and industry on the other the issues are likely to be serious enough to warrant resolution by Ministers. That said it would be inappropriate for Ministers to be responsible for decisions on individual applications such as those related to ICPs.

2. Interception Capability Compliance

- 2.1 The Interception regime is predicated on C/CSPs ensuring the capacity to intercept traffic carried (passing) over their network. The mechanism to achieve this is the previously referred to requirements in Parts 14 and 15 to the Telco Act for C/CSPs to provide reasonably necessary assistance in the execution of a warrant and to ensure that their networks facilities or carriage services are capable of being intercepted in accordance with an interception warrant. The system requiring lodgement of an annual ICP complements these obligations. The scheme as legislated is a confusion of roles and responsibilities; that it works as well as it does is a tribute to agencies and the cooperation given generally by the industry and particularly by Telstra and Optus. However increasingly there are elements of the industry willing to exploit the weaknesses in the legislated scheme and the inherent tension between the national interest in an efficient and competitive telecommunications industry and the national interest in security and law enforcement.
- 2.2 The issue of interception capability compliance was reviewed in the 1999 Telecommunications Interception Review conducted by the Australian Communications Authority (ACA), now the ACMA. That review recommended that the Interception Capability plan process be maintained, that it be supplemented by an interception capability compliance scheme to be developed by the ACA in consultation with the Agency Co-ordinator and the industry and that, if necessary, additional legislative powers be conferred on the ACA to perform this compliance role. The recommendations regarding the capability compliance scheme have not been implemented.

- 2.3 All carriers and nominated carriage service providers (NCSP) are required to lodge ICPs. Since 1999 the number of carriers has grown from 33 to 140. Currently there is only one NCSP. In 2004 a small minority of carriers did not lodge ICPs. These were referred to the ACMA; none have been prosecuted. At present the responsibility for ensuring the lodgement of ICPs resides ultimately with the ACMA. The sanctions available e.g. one million dollars a day, whilst maxima, appear unrealistic.
- 2.4 Any exemption from obligations to provide interception capability poses some risk to national security and law enforcement and granting an exemption is clearly a significant risk management decision.
- 2.5 The Minister for Communications with the written agreement of the Attorney-General may grant an exemption, as can the Agency Co-ordinator. I am advised that the provision for the Minister to grant an exemption is rarely if ever used and that the preferred method is to use the Agency Co-ordinator provision. The ACMA has the power to arbitrate disputes between the Agency Co-ordinator and a carrier. Overwhelmingly, the security and law enforcement agencies believe there is a need for a more effective regime to ensure compliance.
- 2.6 There is also provision whereby the ACMA may grant an exemption for trial services after consulting ‘any appropriate agency’ and being satisfied that the exemption is ‘unlikely to create a risk to national security or law enforcement’. Presumably this provision is intended to recognise the commercial desirability and national interest in trialling new services. Whilst that is accepted the requirement for the ACMA to make the risk judgement, even after consultation, sits oddly with the general scheme of the Part which places effective responsibility with the Attorney-General but leaves the Minister for Communications and, in this

particular instance the ACMA, with apparent accountability. In reality, it is difficult to see how the ACMA could grant such an exemption in the face of advice say by the Agency Co-ordinator that there was such a risk. It would appear more sensible for the decision to rest with the Attorney-General (or the Agency Co-ordinator) having consulted the ACMA.

- 2.7 In the course of the review the ACMA observed that whilst the legislation requires the lodgement of an ICP there is no specific requirement on carriers to implement the plan. Carriers are however required to provide security and law enforcement agencies all reasonably necessary assistance. Under the current scheme it is presumably the ACMA which would decide what is 'reasonable'.
- 2.8 If for no reason other than to ensure that to the greatest extent possible there is a level playing field, there is a need to review the compliance regime to make sure that it is effective in enforcing compliance both with the requirement to lodge ICPs and to implement those if and when required to do so. Any significant gap in the ability to intercept data poses a real risk to security and law enforcement.
- 2.9 The appropriate balance between privacy and access is and always has been properly a matter for government and in the final analysis the Parliament. The same can be said about the balance between the national interests in maintaining a competitive communications industry and those relating to security and law enforcement.
- 2.10 The present arrangements which seek to reflect that balance tend to confuse responsibilities and result in administrative tensions and uncertainties within industry about the priorities to be given to law enforcement obligations which are capable of being exploited by a small number of carriers. Any wording which

imports discretion in the observance of those obligations exacerbates that situation.

- 2.11 In order to provide certainty to industry it would be desirable to make it clear that any legislation providing access to telecommunications for security and law enforcement purposes and any directions and specifications made under that legislation are binding and will be enforced unless an exemption has been granted by the appropriate authority.
- 2.12 The consultative and decision making processes which precede the making of that binding regime should weigh and balance any competing interests.
- 2.13 One way to resolve any administrative uncertainties would be to make the Agency Co-ordinator responsible for enforcing compliance. Such a role would complement the existing exemption processes and would effectively reinforce the obligation to provide access for security and law enforcement purposes. As such it would redress the perception held by a number of interests that security and law enforcement interests are secondary to industry development concerns.
- 2.14 However on balance, and even if Part 15 of the Telco Act is incorporated into new data access legislation, it would seem appropriate for compliance responsibility to remain with the ACMA as the industry regulator, but that it be more accountable for its actions. Provisions should be made for the Agency Co-ordinator to refer any disputed matters to the ACMA with a recommendation as to the action required to resolve the dispute in the interests of security and law enforcement. In the event that the ACMA did not accept that recommendation it would be required to identify why and disclose the reasons for its decision. The Attorney-General would report to Parliament.

- 2.15 **I recommend that the provisions of the Telco Act and the Interception Act regarding the responsibilities of Ministers, Departments and Agencies in relation to exemptions be re-examined and that the exemption process be clearly made the responsibility of the Agency Co-ordinator.**
- 2.16 **I further recommend that responsibility for compliance remain with the ACMA and that an effective compliance scheme be developed in consultation with the Agency Co-ordinator and implemented.**

3. Technology – The Developing Challenges

3.1. Introduction

- 3.1.1. From a security and law enforcement perspective the objective of a telecommunications data access regime is to ensure that within the boundaries described by the need to protect privacy a warrant can be executed and the content of the communications can be obtained and understood, regardless of the technology, and used for the purpose for which it was obtained.
- 3.1.2. The increasing challenges posed by emerging technology, compounded by industry considerations, involve three elements:
- identification;
 - data capture; and
 - understanding.

3.2. Problems of Identification

- 3.2.1. At risk of stating the obvious if a 'service' being used by a suspect cannot be identified it cannot be accessed, at least in real time. There is therefore a need for some system which enables such a service to be identified. The identification must be unique, indelible and available/accessible.
- 3.2.2. In relation to Global System for Mobiles (GSM) this need was intended to be met through the International Mobile Service Identifier (IMSI) which attaches to a Subscriber Identity Module (SIM). The IMSI or SIM allows a GSM service to access the telecommunications network through a particular service provider. The system requires a person purchasing a SIM card to provide proof of identity which is recorded against the card's service number (MSISDN) which is then identifiable. In practice however, SIM cards are issued and traded (often in bulk) both within Australia and overseas, often with no regard to these requirements. They are thus of little use for identification purposes. There has been no real attempt by either the industry, elements of which have enthusiastically promoted the practices, or the regulatory authorities to deal with this problem and indeed it is difficult to see how the situation might now be reversed. To all intents and purposes therefore the SIM card and its associated service number is not an effective method of identification.
- 3.2.3. A potentially more promising system of identifying the user would appear to be attempts to utilise the International Mobile Equipment Identifier (IMEI) which is intended to be a unique electronic serial number allocated to each GSM handset. However in practice multiple IMEIs exist i.e. multiple handsets have the same IMEI. Unlike the SIM problem which now seems insoluble the situation with IMEIs does hold some hope of resolution but it would require determined action

by regulators and carriers with significant public impact. For any system based on IMEIs to be used effectively would also require a different legal approach to the basis for access as it appears that such a system would not meet the requirements of the Interception Act that a warrant must only be issued in relation to a 'service'. If the IMEI system is to be developed it would therefore seem necessary to review the concept of 'service'. Whatever the solution it would be imperative that some system be devised which provides for the effective identification of the means of communication.

3.2.4. Under the named person warrant regime, a warrant may be issued in respect of a person who is alleged to have committed or is likely to commit a prescribed offence or engaged in, or likely to engage in, activities prejudicial to security and who it is believed is using or is likely to use more than one telecommunications service. The warrant is an effective tool to assist with the investigation of targets that use multiple SIMs. In this instance it may be possible to make use of interception based on IMEI as a tool to facilitate interception. I understand that the comprehensive reporting arrangements in the Interception Act currently prohibit interception based on IMEI; however I am of the view that there is a basis to consider the possibility.

3.2.5. **Accordingly, I recommend that priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.**

3.3. The Problems of Data Capture and Understanding

- 3.3.1. I have already commented on what I consider to be the need to review the provisions of Parts 13, 14 and 15 of the Telco Act to ensure that, as they relate to the access of data for national security and law enforcement purposes, they are incorporated into new data access legislation.
- 3.3.2. For interception to remain effective it is essential that the capacity to intercept traffic be maintained and that it be provided by the C/CSPs. This is generally accepted by the industry. The more contentious issue is the nature of the product provided to intercepting agencies by the C/CSP. The ever increasing range of data products carried over networks, often as a service to other providers, means that that data is often not readily interpreted by the carrier. From the point of view of the intercepting agencies receiving the raw data is of little use and defeats the intention of the scheme which pre-supposes product in useable form.
- 3.3.3. **One solution would be to maintain the obligation on C/CSPs by requiring them in turn to impose on service providers for whom they carry data the obligation to interpret that data (or at least the means to decode it) and to provide useable product. I recommend this be done.**
- 3.3.4. However, given the international nature of communications and the developing technology such a scheme is increasingly likely to run into situations where useable intercept of data is not available at least in a timely fashion. A solution might be to establish a central capacity able to interpret such data. Any facility established to provide that capacity would of necessity draw heavily on Commonwealth resources from the Attorney-General's and Defence portfolios. C/CSPs would still be required to provide useable product where practicable and

interception would continue to be practised by intercepting agencies under the interception regime.

3.3.5. A complementary development which has been mooted by some industry elements is the creation of a central interception facility managed by one or more of the major carriers. Whilst such a facility may have real advantages it poses many questions. The centralisation of capacity may itself pose serious risks both physical and in terms of security. Cost recovery would appear likely to be a significant issue for users. Presumably such a facility would only work with the cooperation of all C/CSPs. Whilst it may be possible to re-enforce that cooperation by legislation any such attempt is likely to be strongly resisted. On balance it would appear that whilst the possibility of such a facility should not be rejected it should be left to industry to develop and sponsor, possibly with official encouragement.

4. Cost Implications

- 4.1 I am asked in the course of considering and commenting on the issues to ‘have regard to the cost implications, including cost recovery mechanisms’.
- 4.2 Interception under the current regime and the costs of providing the ability to intercept traditional telephony services are borne by the C/CSP and the costs associated with the format and delivery of actual interception are borne by the agency on the basis that the C/CSP makes neither a profit nor a loss. The detailed arrangements with each C/CSP are contained in ‘contract arrangements’ with all of the agencies.
- 4.3 **In my opinion whilst there may be scope for efficiencies in the ‘contracting’ process this arrangement is appropriate and accordingly, I recommend that it should be maintained.**
- 4.4 In relation to IP and other data networks at least the major carriers accept that it is reasonable for them to meet the costs of providing access to data travelling over a specified data connection. However it is their view that they should not be responsible for interpreting (including extracting, decrypting and analysing) the target communication from that data. They do accept that telecommunication application providers and service providers, including carriers in respect of the applications they provide, should be required to provide ‘reasonable assistance’ with the interpretation of that data but maintain the view that interpretation is the responsibility of the agency.
- 4.5 From the carrier’s perspective the problem arises because with IP and other data networks they are no longer in effective control of all the data being carried over the basic network connection they provide. That connection will increasingly carry ‘packets’ of data for other service providers. In very board terms what is

‘in’ those packets i.e. whether it is voice, text or image and if and how it is encoded, is determined by the provider of the ‘value added services’ which the C/CSP do not necessarily provide and may not be able to interpret. In many cases the carrier will have no knowledge of the customers who may be the target.

4.6 I understand the problem. However I am of the view that to remain effective interception requires that where possible the agency be provided with the content of communications in useable form, that is in a form that can be listened to, increasingly importantly ‘read’, and or recorded and used in evidence. This requires that in addition to the obligation on the carrier to intercept the data, the provider of the ‘value added services’ should be obliged to provide the communication in useable form, or, where for any reason that is not appropriate or even possible, to provide the agency with the means to identify and interpret the data. **I recommend that the carrier and the service provider respectively should bear the costs of meeting those obligations.**

4.7 In my view that distribution of costs best reflects the current model and allocates the costs where they are best able to be managed. It will however almost certainly increase the costs to the C/CSP. It must be anticipated that those increases will be passed on to users but it is those same users who are receiving the benefit of the value added services.

4.8 The other cost regime of major significance in terms of data access is the charges levied by carriers for providing material under the provisions of the Telco Act. Under the present regime carriers are entitled to charge on the basis of no loss/no gain for information they are required to provide to agencies entitled to require information in accordance with sections 282 and 283 of that Act. In my view that regime is appropriate and I recommend that it be continued.

- 4.9 There is however one aspect of cost attribution that I believe does require consideration. There are a number of agencies that can and do make requests for data by virtue of other legislation e.g. the *Social Security (Administration) Act 1999* which makes no provision for payment. A similar issue arises in relation to access required by subpoena or on the order of a Court.
- 4.10 **Accordingly, I recommend that C/CSPs should be entitled to recover their reasonable costs on the basis of the no loss/no gain formula whenever they provide data and the legislation should make that explicit.**
- 4.11 I have in the course of the review, made a number of recommendations that if accepted will impact on the costs of administering the data access scheme for security and law enforcement purposes e.g. abolishing TIRAC see para 8.7. There is little to be gained from repeating the arguments or the recommendations and have therefore confined my comments in this part to matters not covered elsewhere.

5. The Protection of Information Systems

- 5.1 I am asked to specifically comment on the protection of information systems from attack by means of the telecommunications system, including the use of intrusion detection systems and other measures.
- 5.2 This is an aspect which is peculiarly the responsibility of the Minister for Communications. However the wider issue which does concern the Attorney-General's portfolio is the protection of critical national infrastructure one element of which is the telecommunications system.
- 5.3 It is always itself a risk to make statements about particular levels of risk and the likelihood of attacks. However the evidence available to me suggests that the risk of attack on the telecommunications system as such is not high and that in the event of such an attack happening the consequences, although serious, would be manageable because of the redundancy within the system.
- 5.4 That said there is no room for complacency nor on the evidence available is there any. The major providers of services are well aware of the dangers and are employing appropriate detection measures. The Critical Infrastructure Protection Branch of AGD is also well aware of the risks and is active in ensuring that critical infrastructure elements and industry more broadly are properly informed of the risks and encouraged to prepare against the eventuality of major systems failures from whatever cause.
- 5.5 Probably the greatest vulnerability relates to personnel security, and this is an area that does appear to warrant greater attention. It may be that there is a need for C/CSPs as part of the critical infrastructure to provide security plans.

- 5.6 There is also the opportunity through forums such as the LEAC both to educate and reinforce the telecommunications industry specific messages about security generally and personnel security specifically.
- 5.7 **I recommend that the security of information systems as part of the critical national infrastructure continue to be regularly assessed and that personnel security receive particular attention.**

6. The Classification of Offences

- 6.1 In order to obtain an interception warrant in the course of investigating an offence, the offence must meet the requirements of the Interception Act as being either a Class 1 or Class 2 offence. The requirements for Class 1 and Class 2 offences are set out at Attachment 2. The overwhelming view of law enforcement agencies is that the classification system is overly prescriptive and can result in investigators being unable to access data even where the offence is clearly related to a prescribed offence.
- 6.2 The history of amendments to Class 2 offences does not indicate any great demand for change. I understand that the number of amendments does not reflect the requests that have been made by the various agencies. Anecdotally, the agencies also claim that given the immediacy of the investigative processes they often do not pursue amendments once the view is formed in a particular case that interception is not available. They also point to the undesirability of adding more technicalities to the list of offences to cover individual circumstances.
- 6.3 Given that the objective in the case of both Class 1 and Class 2 offences is to justify the issuing of an interception warrant and having regard to the similarity of the offences it is not clear why the distinction is made. Any significance can only be in terms of the processes relating to the issue of a warrant. The only difference between those processes is that in relation to Class 2 offences the issuing authority is required to have regard to the gravity of the offence and the extent of the interference to privacy involved. In the case of Class 1 the gravity of the offences is inherent and presumably is regarded as over-riding any privacy considerations.
- 6.4 In relation to privacy, it could well be argued that, having regard to the stated objective of the Interception Act as being the protection of privacy, in all cases

‘privacy’ is a relevant issue and should be a factor considered by the issuing authority. The fact is of course that privacy considerations are unlikely to preclude the issue of a warrant for any of the offences characterised as Class 1 offences or indeed for many of the Class 2 offences.

6.5 **I recommend that as it produces no meaningful difference in outcome, and adds to the length and complexity of an already convoluted Act, the distinction between Class 1 and Class 2 offences be removed to follow the Class 2 standard issuing requirement.**

6.6 Indeed, and related to the views expressed by law enforcement agencies, unless there are significant offences punishable by imprisonment for a maximum period of at least seven years that it is intended to exclude, there would appear to be no reason why both classes of offences could not be identified simply by reference to the prescribed period of imprisonment. It would of course mean that the States, by establishing the period of imprisonment, would in effect be responsible for identifying the offences which would qualify for an interception warrant but, less obviously, that is to a large extent the current reality: it is hard to imagine arson punishable by a maximum term of imprisonment of seven years that would not be regarded as serious. In any event the gravity of the offence, irrespective of the prescribed term of imprisonment, is a relevant consideration for the issuing authority i.e. a Federal Judge or senior member of the Administrative Appeals Tribunal in the case of the Interception Act.

6.7 It is unlikely that a State government would be tempted to use seven year gaol sentences to significantly and controversially expand the circumstances in which an interception warrant may be issued. However, were a State to do so it would

be immediately obvious through the warrant reporting arrangements and action could be initiated to limit those circumstances if it was considered desirable.

6.8 **Accordingly, I recommend that those offences currently described as Class 1 and Class 2 offences be identified solely by reference to the prescribed term of imprisonment.**

7. Protective Access

- 7.1 Both the Telco Act and the Interception Act presently recognise that some functions related to the provision or operation and maintenance of services need to be exempted from the strict application of the general prohibitions against interception, access and disclosure e.g. acts done by an employee of a carrier in the course of installing equipment or by a person providing an emergency service.
- 7.2 Understandably and properly those exceptions are tightly drawn and tightly controlled.
- 7.3 During the review it became obvious that there are circumstances which are not appropriately catered for by the existing exemptions but which, although different, warrant special consideration.
- 7.4 In the main, those circumstances were related to the need to protect enterprise systems against damage whether deliberate or accidental. An example is the need to protect computer systems against unauthorised entry (hacking) or damage from viruses or worms. Whilst much of this can be achieved through systems applications there is often a need for human intervention which it is argued can involve interception or access in contravention of the relevant legislation.
- 7.5 There are two critical elements to 'interception': the first is the concept of the communication 'passing over' the system and the second is 'the system' that it is 'passing over'. The concept of 'passing over' has received a lot of attention and I think is effectively resolved by acceptance of the idea of the communication being automatically processed as electromagnetic energy up to the point at which it can be directly accessed by the intended recipient. However the issue of 'direct access' does itself raise some issues about whether a communication is still

‘passing over’ the system and therefore subject to the Interception Act when it has been ‘downloaded’ but which, on its way to the recipient, is processed by equipment say a ‘firewall’ installed by the recipient or more contentiously, an employer to protect their equipment, and as a consequence is viewed by an authorised person as part of that process.

- 7.6 It is at least arguable that once such communications reach the equipment installed by the ‘owner’ to protect their equipment they are no longer ‘passing over the system’ or even within the system. If that were so they would no longer be subject to either the Telco Act or the Interception Act.
- 7.7 If however such communications are still ‘passing over the system’ access would require an interception warrant. If they are not passing over the system but are still ‘within’ the system they would be treated as stored data. At the moment as stored data access would be in accordance with the Telco Act.
- 7.8 The submissions were overwhelmingly opposed to access to such communications being governed by the Interception Act. I agree. Even as stored communications the requirements of the Telco Act would appear to effectively preclude access for the intended purpose, i.e. the protection of the system.
- 7.9 The implications for the effective protection of systems if access is denied are serious including for very large users such as the States and the Commonwealth. The Department of Defence advises that without speedy access to the data major systems will be at risk with implications for essential functions and for costs. The current exclusion of stored data from the Interception Act is seen as enabling that speedy access.

- 7.10 Given the 'rights' of owners to protect their system, the potential consequences of not doing so, the universality of the need and the time-critical nature of the required response, it is not in my opinion possible to meet the reasonable needs to protect systems by amending the Interception Act to provide specific exemptions.
- 7.11 However from a privacy point of view uncontrolled access is simply not satisfactory. An access regime should be established which provides appropriate protections and prevents back-door use and access to obtain content. Those protections should in my view restrict access to that required for the identified purpose i.e. the protection of the system. There should be clear authorisation and the persons with that authority should be clearly identified. Those persons should be required to protect the privacy of any data accessed in the same way that the employees of C/CSPs are required to protect data accessed in the course of their employment. The vexed question is what should happen where such access discloses evidence of criminal behaviour. This is similar to the situation previously discussed in relation to section 282. In my view in both situations the content of the communication should be protected but the person with access may report their view that there may be evidence of criminality etc. The data, presumably other than voice data, could then be accessed as if it were a stored communication i.e. by search warrant. The question of the use of the content of voice data raises significant evidentiary and other problems and should be separately considered.
- 7.12 There are also situations where agencies (often government) incidentally gain access to telecommunications in the course of their normal activities e.g. in developing and/or testing new technologies. Such access is not always authorised by the legislation. Not infrequently the only way to avoid such incidental access

would be to cease the development or forgo the testing with potentially serious consequences for essential projects or alternatively to rely on inadequate simulated testing.

7.13 This latter problem is not peculiar to the area of telecommunications. For example the *Radiocommunications Act 1992* (the Radcomms Act) deals with a similar problem. That Act provides as follows:

24 Defence research and intelligence

- (1) This Act does not apply to anything done or omitted to be done by a member of the Defence Force, or by an officer of the Department of Defence, in the performance of his or her functions or duties as such a member or officer in relation to the operation of an organisation:
 - (a) that is part of the Defence Force or part of the Department of Defence; and
 - (b) the purpose of which relates to:
 - (i) research for purposes connected with defence; or
 - (ii) intelligence.
- (2) This Act does not apply in relation to anything done or omitted to be done by or on behalf of:
 - (a) the Australian Secret Intelligence Service; or
 - (b) the Australian Security Intelligence Organisation.

25 Special defence undertakings

This Act does not apply to anything done or omitted to be done by a person performing a function or duty in relation to the operation of a facility that is:

- (a) jointly operated by the Commonwealth and a foreign country; and
- (b) a special defence undertaking for the purposes of the *Defence (Special Undertakings) Act 1952*.

26 Additional exemption for defence matters

- (1) Subject to subsection (2), Parts 3.1, 4.1 and 4.2 do not apply to anything done or omitted to be done by a member of the Defence Force, or by an officer of the Department of Defence, if:
 - (a) the act or omission takes place in the performance of one of his or her functions or duties as such a member or officer; and
 - (b) the function or duty concerned is, under the regulations, taken for the purposes of this subsection to be a function or duty that relates to:
 - (i) military command and control; or
 - (ii) intelligence; or
 - (iii) weapons systems.

7.14 Whilst the breadth of the exemptions under the Radcomms Act may not be required in relation to the Interception Act and the need may not be confined to defence and security undertakings there does appear to be a need to provide for some exemption(s) where the interception is incidental to an activity which is related to research or testing conducted by an approved agency or enterprise for purposes related to the essential function of that agency or enterprise. One example is where agencies need to test interception capability. Currently this is done in a controlled environment to avoid contravening the Interception Act. Because the tests are not real time they may not identify problems that arise in the commercial provision of services. Testing real time data would assist agencies to establish whether C/CSPs are meeting their obligations under the Telco Act. Such exemptions could be conditional upon rules governing the protection of data incidentally accessed along the lines previously discussed. Authorisation could be a function of the Agency Co-ordinator and could be reported on by the Inspector-General of Intelligence and Security (IGIS) or some other inspecting body.

7.15 **I recommend that, subject to appropriate controls, access to communications without warrant be permitted where it is necessarily incidental to the protection of data systems or the authorised development or testing of new technologies or interception capabilities.**

8. The Reporting Structure

- 8.1 An illustration of the interception regime from a law enforcement perspective is at Attachment 3.
- 8.2 For reporting purposes the elements in the structure are:
- the requirement for the Chief Officers of State intercepting agencies to inform the AFP Commissioner of the issue of a warrant and to provide a copy of that warrant;
 - the general obligation to properly maintain agency records;
 - the obligation to provide copies of documents and reports to Ministers;
 - the obligation on State Ministers to provide information to the Commonwealth Attorney-General (including copies of warrants and revocations);
 - the obligation on the AFP Commissioner to maintain registers of all warrants;
 - the AFP Commissioner's obligation to deliver the up-to-date registers to the Attorney-General every three months;
 - the requirement for a compliance review of agency records by an independent authority on a regular basis;
 - the reporting from the independent authority to the Minister;
 - the report from the State Minister to the Commonwealth Attorney-General;
 - the reporting obligations of the Commonwealth Attorney-General to the Parliament.
- 8.3 The law enforcement agencies, including the AFP, question the requirement for the AFP to be informed of, and be provided with, copies of all law enforcement warrants and revocations. The role as envisaged requires the AFP to review the

documents provided and identify and draw attention to any deficiencies prior to the execution of the warrant. That was seen to be, and probably was, necessary at the time interception powers were first extended to the States. However, the States have now had very considerable experience with the scheme, comparable to that of the AFP, and are comfortable with their roles. For the reasons identified below, in my opinion the continued involvement of the AFP in this area is neither necessary nor appropriate.

- 8.4 In any event I am advised by the AFP that the deficiencies identified by it in 2004/05 would amount to about 0.2% of connections. The error rate for warrants would be even less.
- 8.5 The process is costly. In 2004/05 State agencies paid in total over half-a-million dollars for the ‘service’. Although the costs are recovered it is an impost on scarce AFP resources and appears to me to be inappropriate in terms of the role of the AFP and its relationships with warrant issuing authorities and other law enforcement agencies. That the warrant comes into force when it is received by or on behalf of the State Commissioner, although it cannot be executed until authorised by the AFP, makes the whole process even more problematic.
- 8.6 That said the process does identify some deficiencies. In the main they relate to the largely technical distinctions between Class 1 and Class 2 offences. If, as is recommended, those distinctions are removed, these problems will be resolved. The other area of noted ‘deficiency’ relates to the identification of more than one person on a warrant. I am advised that this reflects conflicting views about the lawfulness of the practice. That problem is recognised and can only be resolved by settling the law. That should be done, if necessary by amending the

Interception Act to clarify the intention e.g. to make it clear that the intention is that each warrant identifies one person and only one person.

8.7 **Accordingly, I recommend that the involvement of the AFP in those reviewing and authorising roles be discontinued along with the need for the Commissioner to be provided with a copy of warrants issued.**

8.8 The warrants and revocations also form the basis for the registers maintained by the Commissioner. To the extent that those registers are important it would appear to me more appropriate were they to be maintained by other than the AFP. The Agency Co-ordinator in AGD already receives on behalf of the Attorney-General copies of all warrants and revocations which are then entered into a database. If it is considered necessary the Agency Co-ordinator could perform the same checks as are now performed by or on behalf of each Commissioner before the warrant is executed. That process could include AFP warrants. However in my view these checks are not necessary. The Department also presently reviews the registers on a three monthly basis prior to them being submitted to the Attorney-General.

8.9 That review currently has the advantage that it includes those warrants issued on the application of the AFP. However if as I recommend the responsibility for maintaining the registers is transferred to the Agency Co-ordinator that review would no longer be appropriate or necessary.

8.10 There are significant advantages and efficiencies to be gained by making the Agency Co-ordinator responsible for maintaining the registers: such an arrangement would free up AFP resources; avoid what are largely duplicatory processes; reinforce the responsibility and accountability of State and

Commonwealth agencies, and reinforce the legal and policy oversight role of the Agency Co-ordinator.

- 8.11 **Accordingly, I recommend that the Agency Co-ordinator be given responsibility for maintaining the registers of warrants. Given that the reporting requirements are imposed for Commonwealth purposes and that no 'service' is provided I also recommend that no charges be imposed.**
- 8.12 The accuracy of the registers and compliance in terms of the records maintained by Commonwealth agencies would continue to be subject to review by the Commonwealth Ombudsman but that review does not, and in my view should not, go to the question of appropriateness of the warrant. In relation to State agencies the Ombudsman's role is performed by the designated independent state authority.
- 8.13 The NSW Attorney-General, who is the responsible minister, has questioned the need for State Ministers to be provided with copies of warrants, instruments and reports as required by section 35 of the Interception Act given that the only function required of the Minister is to forward them to the Commonwealth Attorney-General. The Minister suggests this function could be performed at officer level. The Minister advises that, in accordance with the complementary State law, he receives, reviews and acts on reports from the NSW Ombudsman (the independent State authority) on compliance by NSW agencies with the Interception Act. The Minister advises that he provides the Commonwealth Attorney-General with a copy of the Ombudsman's report. The implication is that the Minister does not examine the other documents.
- 8.14 Given the detailed obligations imposed by the Act it may be questioned whether the intention of the legislated scheme is being met by the Minister relying,

apparently solely, on the reports of the Ombudsman, given that the Ombudsman is concerned only with compliance with the process.

- 8.15 The Act provides that State Ministers are required to provide to the Attorney-General:
- a copy of the warrant issued to the eligible authority;
 - a copy of an instrument revoking such a warrant; and
 - the written reports provided by the Chief Officer of an agency:
 - every three months, about the use made by the authority of intercepted information and the communication of such information by persons other than officers of the agency; and
 - annually, setting out such information as is required to be set out in the Commonwealth Attorney-General's report to Parliament as can be derived from the records of the agency.
- 8.16 The obligation on the Chief Officer and the Minister to provide those reports to the Commonwealth Attorney-General is contained in the Interception Act which is given effect by the relevant State law.
- 8.17 Whatever else may be said about this elaborate reporting structure it is difficult to see any useful purpose being served by requiring the State Minister to act merely as conduit. It makes even less sense in relation to warrants and revocations given that under the existing arrangements the Commonwealth in the form of the AFP has already received and actioned copies.
- 8.18 The scheme would make more sense if the intention was that the State Minister by forwarding the material to the Commonwealth Attorney-General was endorsing it and thereby accepting responsibility for the actions of the State officers involved.

However whether or not that was the intention the legislation does not make that apparent and that intention is clearly not the understanding of the NSW Minister.

8.19 In my view if that is the intention it should be made explicit and if not, and in the absence of some other explicit and agreed objective, the obligation on the State Minister should be removed.

8.20 Assuming that the recommendation that the current requirement to provide copies of warrants and revocations to the AFP be removed, the Minister's suggestion that copies be made available directly by the agencies to the Attorney-General as is effectively done now, (through AGD), is appropriate, although there may be a need for them to be provided in a more timely manner than is now the case. There should be no suggestion that the agencies are reporting directly to the Attorney-General who is then responsible for their actions. In my opinion that responsibility must rest with the State Minister.

8.21 If the Chief Officers' reports are not required by the Minister, which I would find surprising, nor by the Attorney-General, then that obligation should also be removed. Obviously it would not be appropriate to create an exception for one Minister only. Any change should be general. I have received no submissions on this matter from the other State Ministers.

8.22 **Accordingly, I recommend that the views of other State and Territory Ministers be determined before any decision is made.**

9. The Use and Destruction of Data

- 9.1 Both the Telco Act and the Interception Act prohibit the disclosure of accessed telecommunications data except as prescribed.
- 9.2 The Interception Act provides that ‘restricted record’ which means ‘a record other than a copy that was obtained by means of an interception’, which is no longer required for a ‘permitted purpose’ shall be destroyed. Permitted purpose is defined differently for various agencies but broadly covers the investigation of offences for which warrants have been issued, the making of a decision in relation to proceedings of an agency and the keeping of records. The destruction is supervised and reported on by the Commonwealth Ombudsman or the independent authority in the case of a State.
- 9.3 The Telco Act which is much less prescriptive, provides for the recording of information disclosed in accordance with the Act and for the Privacy Commissioner to monitor compliance by eligible persons (carriers, carriage service providers and a number of data base operators) with the provisions of the Act.
- 9.4 The Interception Act definition of restricted record is curious in excluding a copy of a record even though the definition of ‘record’ includes a copy. Thus it would appear possible for agencies to avoid what appears to be to be the clear intent of the Act simply by copying the ‘record’. This issue was commented on in his report by Mr T. Sherman AO who recommended that the anomaly be removed by requiring the destruction of copies. That recommendation was not accepted although on the documents the reason why is not clear and on enquiry I have been unable to discover any reason other than the practicability of enforcing the obligation to destroy all copies . Whilst I understand that argument, from a

privacy point of view it largely makes a nonsense of the requirement to destroy the original document, although there may be some purpose from the point of view of the evidentiary value of the original. That said, in my view, the destruction of the original now serves little purpose.

9.5 This apparent anomaly to one side the evidence from the law enforcement agencies is that at least some intercepted/accessed data should be kept for purposes which are not presently prescribed. It is argued that such data is an invaluable aid in detecting patterns of behaviour and use in relation to say organised crime. In effect what is proposed (and what is probably happening) is the creation of criminal intelligence data bases.

9.6 I have some sympathy with the argument: it seems to me that the utility of such data bases is obvious. The problem is how to limit and control their use. One way would be to expand the definition of 'permitted purposes' to encompass retention for intelligence purposes in prescribed circumstances. For example in connection with certain classes of organisations or associations involving known suspects where it can be demonstrated that the intelligence is likely to assist in the prevention or investigation of criminal activities. Any such data base would be subject to supervision by a central agency along the lines of the IGIS.

9.7 **Accordingly, I recommend that authorised agencies be permitted to retain identified accessed data for law enforcement purposes subject to the establishment of appropriate controls along the lines suggested.**

10. Data Access for Intelligence Purposes

10.1 During the course of the review the question of accessing data by law enforcement agencies for intelligence purposes was raised on numerous occasions. Any data accessed is likely to have some intelligence value and the value of retaining that data in appropriate circumstances has already been canvassed. The obvious follow-on is whether access should be permitted for intelligence gathering for law enforcement purposes rather than in relation to an identified particular crime. Where organised criminal activity is identified it seems likely that a warrant would be obtainable under the present regime. However there are circumstances where the law enforcement concern is about the possibility of future criminal behaviour or where ‘foreign criminal intelligence’ is involved for example in relation to drug smuggling or commercial illegal fishing, where a warrant in some circumstances would not presently be available. As with the retention of data for intelligence purposes there are circumstances where such access, including interception, would be warranted. It would be necessary for there to be appropriate controls modelled on the need to establish ‘justification’ for a warrant to be issued, for privacy to be safeguarded and for any retention of records to be justified and for those records to be destroyed when they are no longer required. These controls would be similar to those applying to intelligence gathering for security purposes.

10.2 An even more effective solution may be to make the Australian Crime Commission (ACC) a central accessing agency able to act on behalf of other law enforcement agencies and provide them with relevant product. Such a role seems entirely consistent with the intended purpose and structure of the ACC. It would still be necessary to identify the purpose and extent of the power and for there to

be an oversighting body and it may be appropriate to consider expanding the functions of the IGIS to perform this role. Alternatively in relation to foreign intelligence for law enforcement purposes, the role of any facility established to interpret data as previously suggested, might be expanded to include such interceptions.

10.3 **Accordingly I recommend that, subject to appropriate controls being put in place, provision be made that allows authorised agencies to obtain access to telecommunications data for law enforcement intelligence purposes.**

11. Other Emerging Technologies

- 11.1 As identified earlier in this report, emerging telecommunications technologies and applications, the complications of truly international systems, and commercial pressures do, and will increasingly, create problems for accessing data. At the same time security and law enforcement agencies will continue to require access to the greatest extent possible within the technical and legal constraints while new methods of access will be devised.
- 11.2 However as previously identified it is likely that agencies will have to develop and use compensatory techniques to achieve at least some of the material now obtained from the telecommunications system. Those technologies may well involve the use of other, often more intrusive forms of electronic surveillance. Whilst not within my remit there may be advantages, and some risks, in reviewing electronic surveillance generally.
- 11.3 One such area that is presently related to telecommunications is wireless technology. As previously identified communications carried solely by means of radiocommunications (e.g. wireless) are excluded from both the Telco Act and the Interception Act.
- 11.4 The use of wireless technology is growing. Presently, apart from some local area applications, radiocommunications generally interface with the telecommunications system and are accessible at least from that point, under the Acts, as appropriate. However the evidence suggests that in a variety of applications this will not always be so. It appears likely that wireless systems that are more broadly independent of the telecommunications system will be available and in use in the not too distant future.

- 11.5 In principle there seems little difference from a privacy point of view between radiocommunications and telecommunications. However the implications of simply bringing radiocommunications within the purview of the existing Acts or the proposed data access legislation, even if that could be done, are far from clear but have obviously wide implications and would involve consideration of the Radcomms Act and possibly other legislation.
- 11.6 **Accordingly, I recommend that this issue be separately reviewed by the appropriate departments and authorities with particular regard to the need to maintain continuity of access where communications transfer from system to system.**

12. B-Party Interceptions

- 12.1 An area of concern raised by law enforcement agencies is the issue of so called ‘B-Party’ intercepts.
- 12.2 The issue arises where there is evidence that a person, other than a person suspected of involvement in the prescribed crime, the B-Party, is using a telecommunications service for communications which are believed to be relevant to the investigation. The B-Party may simply be a conduit for a relevant communication and may not even be aware of the use being made of them.
- 12.3 I am advised that presently the Interception Act is generally interpreted by the Agencies as not authorising the use of B-Party intercepts.
- 12.4 The relevant provisions of that Act require that the issuing authority be satisfied that:
- there are reasonable grounds for believing that a particular person is using, or is likely to use, the service;
 - information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to assist in connection with the investigation by the agency of a relevant crime in which the person is involved;
- 12.5 Those provisions have been interpreted as enabling the issue of a warrant where the particular person involved in the relevant crime (the A-Party) is ‘using’ the B-Party service to effect communications. What constitutes ‘using’ is determined by the particular circumstances, but for example the frequency or extent of the suspect communications such as calls by the A-Party to the B-Party may warrant an interception. What does seem clear is that a single communication or probably

evidence of a limited number of communications would not justify a warrant. The problem with that position is that it requires the issuing authority to accept that interpretation as the basis for issuing a warrant and although the Federal Court in *John Flanagan v The Commissioner of the Australian Federal Police* has upheld the validity of a B-Party warrant it did not provide any useful analysis of the rationale.

- 12.6 Security and law enforcement agencies argue the need to intercept B-Party communications more widely. However there are obvious and serious privacy implications involved. That said the usefulness of such intercepts in appropriate circumstances is equally obvious.
- 12.7 In my opinion the proposition that there are circumstances which warrant B-Party intercepts is convincing but the privacy implications are such that those intercepts should not depend on non-judicial interpretation of the relevant sections, the meaning of which is certainly open to argument.
- 12.8 What in my view must be prevented is using B-Party intercepts as ‘fishing expeditions’.
- 12.9 Appropriate controls might include a requirement that any agency requesting such a warrant must establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation. The agency should also establish that it cannot be obtained other than by telecommunications interception or the use of a listening device. It is then for the issuing authority to consider that evidence along with any other relevant matters such as the invasion of privacy involved and the gravity of the alleged offence in deciding whether to issue a warrant. Warrants should be for limited periods and the destruction of non-material content in whatever form

should be strictly supervised. The number and justification of B-Party intercept warrants should be separately recorded by the Agency Co-ordinator and reported to the Attorney-General. The use of such warrants should be separately reported to the Parliament.

12.10 **Accordingly, I recommend that the Interception Act be amended to make it clear that B-Party services may be intercepted in limited and controlled circumstances.**

ATTACHMENT 1 – SUBMISSIONS RECEIVED

Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC)
Attorney-General & Minister for Justice – Queensland Government
Attorney-General’s Department of NSW
Attorney-General’s Department, Canberra
Australian Communications & Media Authority
Australian Customs Service
Australian Privacy Foundation
Australian Securities & Investments Commission (ASIC)
Mr Paul Cheffers, Murrumbateman, NSW
Commonwealth Director of Public Prosecutions
Crime & Misconduct Commission, Queensland
Department of Communications Information Technology and the Arts
Electronic Frontiers Australia Inc.
Federation of Ethnic Communities’ Councils of Australia (FECCA)
Ministry for Police – New South Wales
NSW Ombudsman
NSW Police
Office of Police Integrity – Victoria
Office of the Federal Privacy Commissioner
Office of the Victorian Privacy Commissioner
PanAmSat Corporation
SingTel Optus Pty Limited
Tasmania Police
Telstra Corporation Limited
Victorian Ombudsman
Western Australia Police Service

ATTACHMENT 2 – REQUIREMENTS FOR CLASS 1 AND CLASS 2 OFFENCES

Class 1 offence is defined by section 5 of the Interception Act to mean:

- (a) a murder, or an offence of a kind equivalent to murder; or
- (b) a kidnapping, or an offence of a kind equivalent to kidnapping; or
- (c) a narcotics offence; or
- (ca) an offence constituted by conduct involving an act or acts of terrorism; or
- (cb) an offence against Division 72, 101, 102 or 103 of the *Criminal Code*; or
- (d) an offence constituted by:
 - (i) aiding, abetting, counselling or procuring the commission of;
 - (ii) being, by act or omission, in any way, directly or indirectly, knowingly concerned in, or party to, the commission of; or
 - (iii) conspiring to commit;
- an offence of a kind referred to in paragraph (a), (b), (c), (ca) or (cb); or
- (e) an offence constituted by receiving or assisting a person who is, to the offender's knowledge, guilty of an offence of a kind referred to in paragraph (a), (b), (c), (ca) or (cb), in order to enable the person to escape punishment or to dispose of the proceeds of the offence;

and, except for the purposes of an application for a warrant by an agency other than the ACC, includes an offence in relation to which the ACC is conducting a special investigation.

Class 2 offence mean is defined by section 5D of the Interception Act as follows:

- (1) This section sets out the offences that are *class 2 offences* for the purposes of this Act.

Serious offences etc.

- (2) An offence is a *class 2 offence* if:
- (a) it is an offence punishable by imprisonment for life or for a period, or maximum period, of at least 7 years; and
 - (b) the particular conduct constituting the offence involved, involves or would involve, as the case requires:
 - (i) loss of a person's life or serious risk of loss of a person's life; or
 - (ii) serious personal injury or serious risk of serious personal injury; or
 - (iii) serious damage to property in circumstances endangering the safety of a person; or
 - (iiia) serious arson; or
 - (iv) trafficking in prescribed substances; or
 - (v) serious fraud; or
 - (vi) serious loss to the revenue of the Commonwealth, a State or the Australian Capital Territory; or
 - (vii) bribery or corruption of, or by:
 - (A) an officer of the Commonwealth; or
 - (B) an officer of a State; or
 - (C) an officer of a Territory; or

- (viii) the production, publication, possession, supply or sale of, or other dealing in, child pornography; or
 - (ix) consenting to or procuring the employment of a child, or employing a child, in connection with child pornography.
- (2A) Without limiting subsection (2), an offence is also a **class 2 offence** if it is an offence against section 474.19, 474.20, 474.22, 474.23, 474.26 or 474.27 of the *Criminal Code*.

Offences involving planning and organisation

- (3) An offence is also a **class 2 offence** if it is an offence punishable by imprisonment for life or for a period, or maximum period, of at least 7 years, where the offence:
- (a) involves 2 or more offenders and substantial planning and organisation; and
 - (b) involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques; and
 - (c) is committed, or is of a kind that is ordinarily committed, in conjunction with other offences of a like kind; and
 - (d) consists of, or involves, any of the following:
 - (i) theft;
 - (ii) handling of stolen goods;
 - (iii) tax evasion;
 - (iv) currency violations;
 - (v) extortion;
 - (vi) bribery or corruption of, or by:
 - (A) an officer of the Commonwealth; or
 - (B) an officer of a State; or
 - (C) an officer of a Territory;
 - (vii) bankruptcy violations;
 - (viii) company violations;
 - (ix) harbouring criminals;
 - (x) dealings in firearms or armaments;
 - (xi) a sexual offence against a person who is under 16 (including an offence against Part IIIA of the *Crimes Act 1914*);
 - (xii) an immigration offence.

Offences relating to people smuggling with exploitation, slavery, sexual servitude and deceptive recruiting

- (3A) An offence is also a **class 2 offence** if it is an offence against:
- (a) section 73.1, 73.2, 73.3, 73.8, 73.9, 73.10 or 73.11; or
 - (b) section 270.3, 270.6, 270.7 or 270.8; or
 - (c) section 271.2, 271.3, 271.4, 271.5, 271.6 or 271.7;
- of the *Criminal Code*.

Money laundering offences etc.

- (4) An offence is also a **class 2 offence** if it is an offence against any of the following provisions:

- (a) Part 10.2 of the *Criminal Code* (other than section 400.9);
- (aa) section 135.3 of the *Criminal Code*;
- (b) section 73 of the *Confiscation of Proceeds of Crime Act 1989* of New South Wales;
- (c) section 122 of the **Confiscation Act 1997** of Victoria;
- (d) section 64 of the *Crimes (Confiscation of Profits) Act 1989* of Queensland;
- (e) section 563A of *The Criminal Code* of Western Australia;
- (f) section 10b of the *Crimes (Confiscation of Profits) Act, 1986* of South Australia;
- (g) section 67 of the *Crime (Confiscation of Profits) Act 1993* of Tasmania;
- (h) section 74 of the *Proceeds of Crime Act 1991* of the Australian Capital Territory.

Cybercrime offences etc.

- (5) An offence is also a **class 2 offence** if it is an offence against any of the following provisions:
 - (a) Part 10.7 of the *Criminal Code*;
 - (b) section 308C, 308D, 308E, 308F, 308G, 308H or 308I of the *Crimes Act 1900* of New South Wales;
 - (c) section 247B, 247C, 247D, 247E, 247F, 247G or 247H of the **Crimes Act 1958** of Victoria;
 - (d) a provision of a law of a State (other than New South Wales or Victoria) that corresponds to a provision covered by paragraph (a), (b) or (c);
 - (e) a provision of a law of a Territory that corresponds to a provision covered by paragraph (a), (b) or (c);
 - (f) section 440A of *The Criminal Code* of Western Australia.

Offences connected with other class 2 offences

- (6) An offence is also a **class 2 offence** if it is an offence constituted by:
 - (a) aiding, abetting, counselling or procuring the commission of; or
 - (b) being, by act or omission, in any way, directly or indirectly, knowingly concerned in, or party to, the commission of; or
 - (c) conspiring to commit;
 an offence that is a class 2 offence under any of the preceding subsections.

Warrant Reporting	<p>All Agencies</p> <p>[ss.35(1)(b)] Chief Officer shall give to the State Minister:</p> <ul style="list-style-type: none"> ○ copy of each warrant as soon as practicable ○ copy of each revocation as soon as practicable ○ final effectiveness report within 3 months of the cessation of the warrant ○ annual report as soon as practicable and no later than within 3 months of the end of the reporting year <p style="text-align: center;">State Ministers</p> <p>[ss.35(1)(e)] The State Minister provides the above information to the Attorney-General as soon as practicable</p> <p style="text-align: center;">AFP</p> <p>The AFP must maintain a General register of Warrants [s.81A] and Special Register of Warrants [s.82A] that are to be delivered for inspection to the Attorney-General every three months.</p>
--------------------------	---

Record Keeping Inspection	<p>All Agencies</p> <p>[ss.35(1)(h)] An independent inspection authority shall conduct regular inspections of the agency's records, for the purpose of ascertaining the extent of compliance by the officers of the agency with the agency's record-keeping obligations</p> <p>[ss.35(1)(j)] The inspection authority shall report in writing to the State Minister about the results of the inspection, including any relevant contravention</p> <p style="text-align: center;">State Ministers</p> <p>[ss.35(1)(m)] The State Minister must give to the Attorney-General, as soon as practicable after a report on an inspection of the kind referred to in paragraph (j) is given to the responsible Minister, a copy of the report.</p>
----------------------------------	---

Parliamentary Reporting	<p>Attorney-General</p> <p>[S.99] The Attorney-General must, as soon as practicable after each 30 June, cause to be prepared a written report that relates to the year ending on that 30 June that contains the information required by Division 2 of Part IX of the Act</p>
--------------------------------	---