E

Appendix E – Discussion paper

Australian Government
Attorney-General's Department

EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS

A Discussion Paper to accompany consideration by the Parliamentary Joint Committee on Intelligence and Security of a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform

July 2012

Table of Contents

INTRODUCTION

At the forefront of the Government's commitment to Australia is protecting our national security. In recent years terrorism has been an enduring national security threat. The world and our region have suffered numerous major attacks. And significant terrorist plots have been foiled on our soil. We have developed significant national security capability in the fight against terrorism and other enduring threats such as espionage, serious and organised crime, and cyber crime. Our challenge is to ensure that, as Australia evolves as a 21st century society and economy, our national security capability similarly evolves with high levels of agility and adaptability and continues to meet emerging threats.

As Australia advances, so too do threats to our wellbeing. Meeting the challenges of new technologies and methodologies is a key priority for the Australian Government in the national security sphere. Our law enforcement and security capabilities must keep ahead of terrorists, agents of espionage and organised criminals who threaten our national security and the safety of our citizens. So our law enforcement and intelligence agencies must be equipped with contemporary skills and technologies, and backed by necessary powers – coupled with the appropriate checks and balances and oversight mechanisms society rightly demands.

This package of reform proposals, which comprises telecommunications interception reform, telecommunications sector security reform and Australian intelligence community reform, seeks to do just that. The common thread of national security runs through the proposals, which seek to respond to threats from international state and non-state based actors, terrorism, serious and organised crime and cyber crime.

Just as technology and methodology employed by terrorists, agents of espionage and organised criminals adapts and advances so too must the capabilities and powers of our law enforcement and security agencies. In the absence of action, significant intelligence and evidence collection capabilities will be lost providing criminal elements with a technological upper hand.

Telecommunications interception reform recognises that there are significant challenges facing intelligence and law enforcement agencies in accessing communications, particularly in keeping pace with rapid changes in the telecommunications environment. New, emerging and future technologies impact on the ability of these agencies to access communications to collect intelligence and effectively detect and prosecute crimes. The Australian Crime Commission's *Future of Organised Criminality in Australia 2020* assessment reveals that access to highly effective software, ciphers and other methodologies are increasingly being utilised by organised crime to impede detection by law enforcement. Lawful interception, therefore, is the most important tool in the investigation and

prosecution of serious and organised and other technology-enabled crime, and is vital to effectively collect security intelligence. Proposed reforms seek to allow those agencies to utilise modern technologies to maintain effective investigative techniques.

Telecommunications sector security reform seeks to address the national security risks posed to Australia's telecommunications infrastructure. The security and resilience of such infrastructure significantly affects the social and economic well-being of the nation. While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy or alter critical infrastructure and the information held on it. As Australia's telecommunications landscape continues to evolve, it is appropriate and timely to consider how best to manage risks to the data carried and stored on our telecommunications infrastructure to secure its availability and integrity in the long term. The ideas included in this discussion paper build on consultation with industry earlier in 2012 about the most effective way to manage national security risks to telecommunications infrastructure.

Australian intelligence agencies have made a significant contribution to our safety by constant and careful assessment of possible threats. At least four planned terrorist attacks designed to achieve mass casualties on Australian soil have been thwarted by agencies since 11 September 2001. To continue this crucial role, it is imperative that Australia's intelligence agencies remain robust and can effectively deal with the challenges presented by today's and tomorrow's international security environment. Following the 2008 Report of the Review of Homeland and Border Security conducted by Mr Ric Smith AO PSM, the Attorney-General's Department has worked with relevant agencies to determine the powers required to deal with current and future national security challenges. Australian intelligence community reform is about appropriately equipping and enhancing the operational capabilities of these agencies.

This Discussion Paper contains the terms of reference for the PJCIS inquiry at Chapter One, followed by chapters on each of the proposals which comprise the package of proposals. Chapter Two, 'Interception and the TIA Act', deals with telecommunications interception reform and outlines the problems facing law enforcement and intelligence agencies that have arisen from the operation of the *Telecommunications (Interception and Access) Act 1979.* Chapter Three, 'Telecommunications Sector Security Reform' considers possible amendments to the *Telecommunications Act 1997* to establish a risk based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure. Chapter Four considers ideas for reform of the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001.*

Although the package is referred to the PJCIS in its totality, in considering the ideas the Attorney-General has organised the proposals in three separate groupings: those the Government wishes to progress, those the Government is considering, and those on which the Government expressly seeks the PJCIS' views. Chapter One elaborates on the content of each group. Chapters Two, Three and Four refer to the groups within which the ideas sit, as determined by the Terms of Reference.

CHAPTER ONE

TERMS OF REFERENCE - INQUIRY INTO POTENTIAL REFORMS OF NATIONAL SECURITY LEGISLATION

Having regard to:

- the desirability of comprehensive, consistent and workable laws and practices to protect the security and safety of Australia, its citizens and businesses,
- the need to ensure that intelligence, security and law enforcement agencies are equipped to effectively perform their functions and cooperate effectively in today's and tomorrow's technologically advanced and globalised environment, and
- the fact that national security brings shared responsibilities to the government and the private sector:

1) The Parliamentary Joint Committee on Intelligence and Security is to inquire into potential reforms of National Security Legislation, as set out in the attachment and which include proposals relating to the:
   a) *Telecommunications (Interception and Access) Act 1979*
   b) *Telecommunications Act 1997*
   c) *Australian Security Intelligence Organisation Act 1979*
   d) *Intelligence Services Act 2001*

2) The inquiry should consider the effectiveness and implications of the proposals to ensure law enforcement, intelligence and security agencies can meet:
   a) the challenges of new and emerging technologies upon agencies' capabilities
   b) the requirements of a modern intelligence and security agency legislative framework, and to enhance cooperation between agencies, and
   c) the need for enhancements to the security of the telecommunications sector.

3) The Committee should have regard to whether the proposed responses:
   a) contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector
   b) apply reasonable obligations upon the telecommunications industry whilst at the same time minimising cost and impact on business operations in the

telecommunications sector and the potential for follow on effects to consumers, the economy and international competition, and

c) will address law enforcement reduction of capabilities from new technologies and business environment, which has a flow-on effect to security agencies.

4) The Committee should take account of the interests of the broad range of stakeholders including through a range of public, *in camera* and classified hearings.

5) The Committee should provide a written report on each of the three elements of the National Security Legislation referral to the Attorney-General.

The National Security Legislation the subject of the inquiry has three different elements and Objectives. They relate to:

- modernising lawful access to communications and associated communications data
- mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers, and
- enhancing the operational capacity of Australian intelligence community agencies.

The proposals across the three different packages are separated into three different groupings:

A. those the Government wishes to progress

B. those the Government is considering progressing, and

C. those on which the Government is expressly seeking the views of the PJCIS.

A - Government wishes to progress the following proposals:

Telecommunications (Interception and Access) Act 1979

1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). This would include the examination of:

    a. the legislation's privacy protection objective

   b. the proportionality tests for issuing of warrants

   c. mandatory record-keeping standards

   d. oversight arrangements by the Commonwealth and State Ombudsmen

2. Reforming the lawful access to communications regime. This would include:

   a. reducing the number of agencies eligible to access communications information

   b. the standardisation of warrant tests and thresholds

3. Streamlining and reducing complexity in the lawful access to communications regime. This would include:

   a. simplifying the information sharing provisions that allow agencies to cooperate

   b. removing legislative duplication

4. Modernising the TIA Act's cost sharing framework to:

   a. align industry interception assistance with industry regulatory policy

   b. clarify ACMA's regulatory and enforcement role

Australian Security Intelligence Organisation Act 1979

5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions

   a. to update the definition of 'computer' in section 25A

   b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.

6. Modernising ASIO Act employment provisions by:

   a. providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'

   b. Making the differing descriptions ('officer,' 'employee' and 'staff') denoting persons as an 'employee' consistent

c. Modernising the Director-General's powers in relation to employment terms and conditions

d. Removing an outdated employment provision (section 87 of the ASIO Act)

e. Providing additional scope for further secondment arrangements

Intelligence Services Act 2001

7. Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies.

B. Government is considering the following proposals:

Telecommunications (Interception and Access) Act 1979

8. Streamlining and reducing complexity in the lawful access to communications regime – this would include:

   a. Creating a single warrant with multiple TI powers

9. Modernising the Industry assistance framework –

   a. Implement detailed requirements for industry interception obligations

   b. extend the regulatory regime to ancillary service providers not currently covered by the legislation

   c. implement a three-tiered industry participation model

Australian Security Intelligence Organisation Act 1979

10. Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.

11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

    a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.

b. Align surveillance device provisions with the Surveillance Devices Act 2007

c. Enable the disruption of a target computer for the purposes of a computer access warrant

d. Enable person searches to be undertaken independently of a premises search

e. Establish classes of persons able to execute warrants

12. Clarifying ASIO's ability to cooperate with the private sector.

13. Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.

C. Government is expressly seeking the views of the Committee on the following matters:

Telecommunications (Interception and Access) Act 1979

14. Reforming the Lawful Access Regime
    a. expanding the basis of interception activities

15. Modernising the Industry assistance framework

    a. establish an offence for failure to assist in the decryption of communications

    b. institute industry response timelines

    c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

Telecommunications Act 1997

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:

    a. by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference

    b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs

c. Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers

d. Creating appropriate enforcement powers and pecuniary penalties

Australian Security Intelligence Organisation Act 1979

17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:

a. Using third party computers and communications in transit to access a target computer under a computer access warrant.

b. Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant

c. Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry.

d. Introducing an evidentiary certificate regime.

Intelligence Services Act 2001

18. Amending the Intelligence Services Act to:

a. Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities.

b. Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required.

c. Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

CHAPTER TWO

INTERCEPTION AND THE TIA ACT

1. Introduction

The primary objective of the current legislation governing access to communications is to protect the privacy of users of telecommunications services in Australia by prohibiting covert access to communications except as authorised in the circumstances set out in the TIA Act.

The exceptions to the general prohibition against interception recognise the need for national security and law enforcement agencies to access the information necessary to protect community safety and security. The limited focus of the exceptions reflects Parliament's concern to balance the competing right of individuals to freely express their thoughts with the right of individuals to live in a society free from threat to personal safety.

Interception of telecommunications content and data is a powerful and cost effective tool for law enforcement and security agencies to reduce threats to national security and to assist in the investigation and prosecution of criminal offences.[1] Access to interception is tightly regulated and, in relation to content, is limited to the investigation of serious offences under the authority of an independently issued warrant and subject to a range of oversight and accountability measures.

However, the interception regime provided by the current Act reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the Act was made. Many of these assumptions no longer apply, creating significant challenges for agencies in using and maintaining their investigative capabilities under the Act.

In the absence of urgent reform, agencies will lose the ability to effectively access telecommunications, thereby significantly diminishing the collective ability to detect, investigate and prosecute threats to security and criminal activity.

The Government is therefore considering the need for a new interception regime that better reflects the contemporary communications environment and is seeking the views of the Committee on the content of that regime. Priority issues for consideration by the Committee are set out in the Terms of Reference, grouped into:

[1] See *Report of the Review of the regulation of access to communications* (2005) (the Blunn Report) at http://www.ag.gov.au/Publications/Pages/BlunnreportofthereviewoftheregulationofaccesstocommunicationsAugust2005.aspx

- Matters the Government wishes to progress;
    - Examining the legislation's privacy protection objective, the proportionality test for issuing warrants, mandatory record-keeping standards, and oversight arrangements by the Commonwealth and State Ombudsmen
    - Reducing the number of agencies eligible to access communications information
    - Standardising warrant tests and thresholds
    - Simplifying the information sharing provisions that allow agencies to cooperate
    - Removing legislative duplication
    - Aligning industry interception assistance with industry regulatory policy
    - Clarifying the AMCA's regulatory and enforcement role
- Matters the Government is considering
    - Creating a single warrant with multiple TI powers
    - Implementing detailed requirements for industry interception obligations
    - Extending the regulatory regime to ancillary service providers not currently covered by the legislation
    - Implementing a three-tiered industry participation model; and
- Matters on which the Government expressly seeks the views of the Committee.
    - Expanding the basis of interception activities
    - Establishing an offence for failure to assist in the decryption of communications
    - Instituting industry response timelines
    - Applying tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts

This chapter of the discussion paper describes the role played by access to communications content and data in protecting the community from threats to security and serious crime, summarises the key features of the current legislative regime and the challenges it is facing. The chapter concludes by suggesting that, to achieve a legislative regime that is effective in the contemporary communications environment, reforms may be developed to:

- Strengthen the safeguards and privacy protections of the interception regime in line with contemporary community expectations;
- Reform the lawful access regime for agencies;
- Streamline and reduce complexity in the lawful access regime; and
- Modernise the cost sharing framework.

1.1 Effectiveness of lawful covert access to communications

Lawful interception and access to telecommunications data are cost-effective investigative tools that support and complement information derived from other methods.

In 2010-2011 there were 2441 arrests, 3168 prosecutions (2848 for serious offences) and 2034 convictions (1854 for serious offences) based on lawfully intercepted material.[2] Law enforcement agencies made 91 arrests, 33 prosecutions and obtained 33 convictions based on evidence obtained under stored communications warrants.[3]

These figures may underestimate the effectiveness of interception because a conviction can be recorded without entering the intercepted material into evidence.[4] Interception also allows agencies to identify criminal connections, co-conspirators and organised crime associates and assists in establishing the methodology of criminal enterprises. It also plays an important role in identifying child exploitation material, sexual slavery and terrorist organisations. The figures are specific to law enforcement agencies and do not take into account the use of intercepted information by ASIO in carrying out its functions (which is reflected in ASIO's classified annual report).

Telecommunications data is commonly the first source of important lead information for further investigations and often provides a unique and comprehensive insight into the behaviour of persons of interest.

1.2 The national security environment

Under the TIA Act, the Australian Security Intelligence Organisation (ASIO) can ask the Attorney-General to issue an interception warrant in order to investigate activities prejudicial to security or to collect foreign intelligence.

Australia is, and will remain, a terrorist target for the foreseeable future with jihadist terrorism being the most immediate threat.[5] The threat of a terrorist attack in Australia or

[2] AGD, *TIA Act Report for the year ending 30 June 2011*, p. 46.

[3] AGD, *TIA Act Report for the year ending 30 June 2011*, p. 60.

[4] AGD, *TIA Act Report for the year ending 30 June 2011*, p. 47.

[5] ASIO, *ASIO Report to Parliament 2010-11*, p. xviii.

against Australian interests overseas remains real.[6] Since 2001, four mass casualty attacks within Australia have been disrupted because of the joint work of intelligence and law enforcement agencies.[7]

Since 2001, 38 people have been prosecuted in Australia as a result of counter-terrorism operations and 22people have been convicted of terrorism offences under the *Criminal Code Act 1995* (the Criminal Code).[8]

Intercepted information has played an important role in recent counter-terrorism prosecutions and in preventing planned terrorist attacks. In 2008, several men who faced trial in Melbourne were convicted of being a member of a terrorist organisation. The evidence that the group was engaged in preparing or fostering a terrorist act was largely contained in 482 intercepted conversations that were put before the jury. Some of these communications were covertly recorded in the home of the organisation's leader.

While terrorism is a key issue, the *ASIO Report to Parliament 2010-11* notes that espionage is an enduring security threat to Australia, both through the traditional form of suborning persons to assist foreign intelligence agencies and new forms such as cyber espionage. Nation states, as well as disaffected individuals and groups, are able to use computer networks to view or siphon sensitive, private or classified information for the purpose of espionage, political, diplomatic or commercial advantage. As the actors involved undertake this activity within 'cyberspace', the lawful interception of their communications is often a crucial aspect of any investigation aiming to resolve the nature of the activity and the identity of the perpetrators.

1.3 Serious offences and serious contraventions – Commonwealth and State

The precursor to the TIA Act focused on national security but with the emerging national drug crisis in the 1970s the current Act was passed to ensure that interception powers were also available to the Australian Federal Police to investigate narcotic offences. Since its enactment the TIA Act has been amended to allow a broader range of law enforcement agencies to intercept communications to investigate other serious offences.

Under the TIA Act, serious offences generally include Commonwealth, State and Territory offences punishable by imprisonment for seven years or more. Particular examples of serious offences for which interception can be obtained are murder, kidnapping and offences involving serious personal injury. There are also a range of other offences defined

[6] ASIO, *ASIO Report to Parliament 2010-11*, p. ix.

[7] ASIO, *ASIO Report to Parliament 2010-11*, pp. xviii, 5.

[8] PM&C, *Counter-Terrorism White Paper*, 2010, p. 7.

as serious offences in the TIA Act where the use of the Australian telecommunications system is integral to the investigation of the offence.[9]

According to the Australian Institute of Criminology (the AIC), in 2010 there were 260 victims of homicide in Australia. There were also:

- 171,083 victims of assaults,
- 17,757 victims of sexual assaults; and
- 14,582 victims of robberies[10]

1.4 Organised crime

An interception warrant can also be sought to detect, investigate, prevent and prosecute persons involved in organised crime. Serious and organised crime refers to offences that involve two or more offenders, require substantial planning and organisation and the use of sophisticated methods and techniques and are committed in conjunction with other serious offences.

The Australian Crime Commission (ACC) in its 2010 report *Organised Crime in Australia,* assessed the overall threat to Australia from organised crime as "High", [11] estimating the cost of such crime at $10 to $15 billion per year.[12]

The rapid adoption of telecommunications technology and high speed broadband internet has the potential to increase high-tech crime in Australia, including both the use of technology to facilitate traditional crime and specific crimes directed at information and communication technologies.[13] High tech crime covers a range of offences such as identity crime, sales of illicit products, credit card fraud, money laundering and child exploitation material.

The individuals involved in many of these activities are highly sophisticated in their operations using multiple technologies and frequently changing their methodology to avoid detection. Their adaptiveness means that the tools available under the interception regime provide the only investigative technique capable of identifying and disrupting their activities, many of which are conducted at the global level.

---

[9] See s 5D of the TIA Act.

[10] AIC *2011Australian crime:Facts & figures* http://www.aic.gov.au/documents/0/B/6/%7B0B619F44-B18B-47B4-9B59-F87BA643CBAA%7Dfacts11.pdf, p2.

[11] ACC, *Organised Crime in Australia 2011*, http://www.crimecommission.gov.au/sites/default/files/files/OCA/2011/oca2011.pdf, p. 7.

[12] ACC, *Organised Crime in Australia 2011*, p. 3.

[13] ACC, *Organised Crime in Australia 2011*, p. 25.

Over the past 18 months, information obtained through interception activities in relation to a single money laundering investigation has helped the AFP to arrest 35 offenders and to seize 421 kilograms of drugs and over $8,000,000 in cash.

Many transnational crimes, such as money laundering, also pose a threat to Australia's national security interests with clear links between the proceeds of such crimes and the funding of terrorist activities overseas.

1.5 Fundamentals of the current Act

Research suggests that access to and the use of intercepted information will continue to play an important role in supporting the functions of national security and law enforcement agencies. The conduct of national security and law enforcement investigations demonstrates that lawful interception is a critical capability that cannot be replaced by other investigative methods.

In the thirty years since its inception, the TIA Act has been able to accommodate emerging threats and changes in criminal behaviour because the legislation does not limit the concept of interception to a particular technology (such as a telephone). By couching the Act this way the currency of the legislation has been maintained through amendments that have clarified the application of the Act as the telecommunications environment and what is necessary for agencies to properly protect the community have changed.

Towards a new approach

The pace of change in the last decade has meant the Act has required frequent amendment resulting in duplication and complexity that makes the Act difficult to navigate and which creates the risk that the law will not be applied as Parliament intended.

Much of the need to amend the TIA Act stems from the contextual foundations of the Act.

Many of those foundations no longer apply, creating significant challenges for agencies to maintain current investigative capabilities. Agencies continue to adapt their capabilities within the constraints of the current legal framework but this has not ameliorated the impact of the rapid changes in the telecommunications environment and the ability of agencies to access communications.

In recent years there have been significant advancements in technology and changes to industry structure, practices and consumer behaviour. The communications landscape of the 1970s which was dominated by a single provider and focused on communications made by telephone no longer exists.

The magnitude of change to the telecommunications environment suggests that further piecemeal amendments to the existing Act will not be sufficient. Rather, holistic reform that

reassesses the current assumptions is needed in order to establish a new foundation for the interception regime that reflects contemporary practice.

Telecommunications in 2012

When the TIA Act was enacted, an agency could expect that it would be able to lawfully intercept most, if not all, of a person's communications. Today, changes in the way communications technology is delivered and used mean that the expectation is much lower.

At the end of June 2011, there were 287 fixed-line telephone service providers, three mobile network operators, 176 Voice over Internet Protocol (VoIP) service providers, 33 satellite providers and 97 Internet Service Providers (only including ISPs with at least 1000 subscribers).[14]

Together they provided 29.28 million mobile services and 10.54 million fixed-line telephone services and supported some 10.9 million internet subscribers.[15] Around 12.7 million Australians (69% of the population) had access to a broadband internet connection at home, while around 3.9 million Australians (21% of the population) accessed the internet from their mobile phone.[16]

Australian consumers are increasingly accessing multiple technologies and services to communicate. As at June 2011, 57% of Australians were using at least three communications technologies (fixed-line telephone, mobile phone and internet) and 26% of adults were using at least four communications technologies (fixed line telephone, mobile phone, VOIP and the internet).[17]

There has also been a trend towards high speed internet services, with the proportion of internet subscribers on services of eight megabits per second or more increasing from 26% to 33% in 2009-10.[18] The increase in internet speed has resulted in a rise in data downloads. The average user downloaded 25.1 gigabytes of data in the June quarter of 2011, 56% more than in the June quarter of 2010.[19]

In the June 2011 quarter, Australians downloaded 274,202 terabytes of data from fixed-line wireless internet services, an increase of 76% from the June 2010 quarter. Fixed-line broadband accounted for 254,947 terabytes (around 93%), while wireless broadband

[14] ACMA, *Communications report 2010-11*, p. 24.

[15] ACMA, *Communications report 2010-11*, p. 25.

[16] ACMA, *Communications Report 2010-11*, p. 18.

[17] ACMA, *Communications report 2010-11*, p. 153.

[18] ACMA, *Communications Report 2009-10*, p. 15.

[19] ACMA, *Communications Report 2010-11*, p. 17.

accounted for 19,194 terabytes (around 7%). There was an additional 3,695 terabytes of data downloaded on mobile handsets in the June 2011, an increase of 415% on the June 2010 quarter.[20]

Along with the increased use of multiple technologies, mobile phones are becoming a 'truly converged consumer device'.[21] The availability of iPhone and Smartphone technology has allowed handset models to offer a number of services including voice, SMS, internet access, email, e-payment, video, music, photography, GPS, VOIP and access to social networking sites. In 2010, smartphones represented 43% of all mobile phones sold in Australia.[22]

Increased network coverage, speed and availability have allowed consumers to access VOIP services more effectively. This technology involves communicating and transporting voice messages over the internet, rather than via the public switched telephone network. VOIP is available on many smartphones and internet devices, so mobile phone users can make calls or send text messages over the internet. VOIP usage in Australia has increased from 2.9 million users in June 2010 to 3.8 million users in June 2011.[23] In the year leading up to June 2011, mobile VOIP usage increased by 226%, with 274,000 users in June 2011.[24]

Social media use has also increased, resulting in more user generated content and providing alternative communication channels to traditional voice services. During June 2011, 8.6 million Australians accessed online social network sites from home, compared to 8.0 million during July 2010.[25]

These trends are expected to continue. In addition, the implementation of the NBN is likely to increase the amount of material that can be accessed through telecommunications devices, encourage competition and technological and service innovation, and drive further industry restructuring. Work on the NBN rollout is planned to commence in over 1500 communities and pass 3.5 million premises throughout Australia by 30 June 2015 and is scheduled to be completed by 2021.[26]

---

[20] ACMA, *Communications Report 2010-11*, p. 26.

[21] ACMA, *Communications report 2009-10*, p. 147.

[22] The Australian, 'Apple's iPhone leads Australia's huge smartphone growth', 15 March 2011, http://www.theaustralian.com.au/australian-it/apples-iphone-leads-australias-huge-smartphone-growth/story-e6frgakx-1226021287594

[23] ACMA, *Communications report 2010-11*, p. 25.

[24] ACMA, *Communications report 2010-11*, p. 16.

[25] ACMA, *Communications report 2010-11, p. 26*.

[26] NBN Co. Media Release, 29 March 2012 at http://www.nbnco.com.au/news-and-events/news/nbn-co-announces-three-year-rollout-plan.html

Legacy assumptions

The complexity of the contemporary communications environment is not reflected in the current interception regime which instead assumes that:

1. Communications to be intercepted are easily identified;
2. A stream of traffic to be intercepted can be isolated from the rest of the communications passing over the network;
3. Carriers and carriage service providers (telecommunications companies and internet service providers) control the traffic passing over their networks;
4. Carriers and carriage service providers are the only entities which control public telecommunications networks;
5. Intercepted communications are easily interpreted or understood;
6. There are reliable sources of associated communications data that link people with identifiers and identifiers to communications; and
7. A 'one size' approach to industry obligations is appropriate.

These assumptions mean the TIA Act takes a technical approach to defining when an interception takes place which was appropriate to the prevailing technologies of the 1960s and 1970s but, with the rise of internet protocol communications, now causes uncertainty about the scope of the general prohibition against interception and fails to recognise the particular demands created by a diverse telecommunications sector.

2.1 Problems with the current approach

The limitations created by the assumptions inherent in the TIA Act impact on the capacity of agencies to:

1. Reliably identify communications of interest and to associate them with telecommunications services;
2. Reliably and securely access communications and associated data of interest within networks; and
3. Effectively interpret the communications to extract the intelligence or evidence

Identifying communications

The TIA Act is based on an assumption that there is a unique, non-ambiguous identifier, such as a phone number, linking the target of an interception warrant to the service (or device) to be intercepted and in turn to the carrier required to give effect to the warrant.

However, typically there are no longer clear, one-to-one relationships between the target of an interception warrant, telecommunications services used by the person, and telecommunications service providers because users of telecommunications services may have multiple 'identities', each of which may only be meaningful to a particular service provider.

Persons seeking to avoid surveillance commonly exploit this situation.

Access to communications content and communications data

The TIA Act is also based on the assumption it is possible to reliably access communications which are the subject of an interception warrant at a convenient point on a carrier's network through which the data must flow. This is problematic as most networks are now based on Internet protocol (IP). With this technology users can access communications via multiple access technologies (fixed networks, wireless, satellite, etc.), multiple physical locations and multiple access service providers, some part of which need not be owned, operated or accessible to regulated participants in the telecommunications industry, such as carriers and carriage service providers (or C/CSPs). As a result, communications cannot be guaranteed to pass over any particular path and therefore it may be necessary to attempt to direct the communications over a particular path to facilitate interception.

In addition, whereas telecommunications services were once provided by a single carrier, in many cases now each communication event typically involves a number of service providers. In a single communications session, a person may access many application services such as a Google search engine portal, a webmail account, a Facebook account, and an online storage repository. Each of these services is provided by a different service provider under separate subscriber accounts and with different unique subscriber 'identities'. In general, the ISP and the access service providers have no knowledge of the application services passing over their infrastructure. Further, many application service providers operate from offshore making the provision of assistance to Australian agencies challenging.

Currently, authorised access to telecommunications data, such as subscriber details, generated by carriers for their own business purposes is an important source of information for agencies. As carriers' business models move to customer billing based on data volumes rather than communications events (for example number of phone calls made), the need to retain transactional data is diminishing. Some carriers have already ceased retaining such data for their business purposes and it is no longer available to agencies for their investigations.

At least part of the complexity can be ascribed to changes in the telecommunications industry. It is no longer possible to always be able to clearly identify the industry participant

with a single target 'identity'. The ready availability of anonymous pre-paid services, inter-carrier roaming agreements, resold services, calling cards and on-line facilities to subscribe to new services all make it necessary for agencies to seek data from multiple providers to ascertain whether any data exists.

Interpreting communications and communications data

All of these variables, particularly when combined with increased data flows and volumes, mean it is now extremely complex and costly to reliably identify and access communications.

Furthermore, once a communication has been accessed, its content is not necessarily clear. In IP-based communications, the content of communications is embedded in data packets in a form which is not readily able to be reconstructed and interpreted outside of the transmitting and receiving terminal devices and the applications running on them. Data used to route, prioritise and facilitate the communications is also embedded along with the content, in the communications packets. This means that agencies must further process communications accessed under an interception warrant to extract and reconstruct the content.

The use of encryption and propriety data formats and typically large data volumes, makes reconstructing communications into an intelligible form difficult for agencies.

2.2 Creating a contemporary regime

In order to preserve the effectiveness of lawful covert access to electronic communications as an investigative tool in the face of rapid developments in technology and the globalisation of the telecommunications industry, the assumptions underpinning the current legislative framework need to be reassessed to ensure they reflect the contemporary communications environment. Realigning the foundations of the regime will address key operational challenges.

Four main areas have been identified as requiring review:

1. Strengthening the safeguards and privacy protections in line with contemporary community expectations;
2. Reforming the lawful access regime for agencies;
3. Streamlining and reducing complexity; and
4. Modernising the cost sharing framework

Strengthening the safeguards and privacy protections in line with contemporary community expectations

Historically, the TIA Act has protected the privacy of communications by prohibiting interception except as allowed under the Act.

Over time the position of privacy in the interception regime has been affected by the balancing inherent in the Act between protecting privacy and enabling agencies to access the information necessary to protect the community. Where the balance between these objectives should lie is left to Parliament to decide.

The need to amend the Act to adapt to changes in the telecommunications environment has seen the range of exceptions to the general prohibition grow. Accordingly, it may be timely to revisit whether the privacy framework within the Act remains appropriate.

As people's use and expectations of technology have changed since the TIA Act was enacted in 1979, so community views about the types of communications that can be accessed and the purposes for which they can be accessed may also have changed.

Reviewing the current checks, balances and limitations on the operations of interception powers will ensure that the privacy needs of contemporary communications users are appropriately reflected in the interception regime.

Consideration is also being given to introducing a privacy focused objects clause that clearly underpins this important objective of the legislation and which guides interpretation of obligations under the Act. By taking these steps, the legislation will be positioned to meet the objective of protecting the privacy of Australian communications from unlawful access.

Reforming the lawful access regime

Telecommunications interception and access to communications data are unique and fundamental tools that cannot be replaced by other investigative techniques. They are cost effective, timely, low risk and extremely successful tools in obtaining intelligence and evidence. Substantial and rapid changes in communications technology and the business environment are rapidly eroding agencies' ability to intercept. Adapting the regime governing the lawful access to communications is a fundamental first step in arresting the serious decline in agencies' capabilities.

The TIA Act provides for four warrants for law enforcement agencies to access content. Three warrants relate to accessing real-time content and one warrant relates to accessing 'stored communications' (which includes emails and text messages accessed from the carrier after they have been sent).

Real-time content based warrants are available to 17 Commonwealth and State and Territory agencies. ASIO's ability to intercept communications supports its functions relating to security. The AFP and State and Territory police forces have access to interception powers as part of a nationally consistent approach to combating serious crime. The remaining agencies are a mix of agencies whose functions relate to investigating police integrity, anti-corruption and serious and organised crime.

While traditionally limited to an offence that carries a penalty of at least 7 years' imprisonment (a 'serious offence'), over time numerous legislative amendments have confused the policy in relation to the circumstances in which interception is available. There are occasions where the general penalty threshold is too high to cover a range of offences for which it is already recognised that general community standards would expect interception to be available. For example, child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks (including offences committed using a computer or involving telecommunications networks) do not meet the general 7 year imprisonment policy threshold.

The stored communications regime allows 'enforcement agencies' (criminal law enforcement agencies, civil penalty enforcement agencies and public revenue agencies) to access the content and associated data of a communication held by a carrier. In addition to interception agencies, enforcement bodies include a range of regulatory bodies such as the Australian Customs and Border Protection Service, the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, the Australian Taxation Office, Centrelink and a range of State and Territory government organisations.

A stored communications warrant can only be issued for the investigation of an offence carrying a penalty of at least three year's imprisonment or a fine of 180 penalty units. The threshold for access is lower than for interception because it was considered at the time the provisions were introduced that communicants often have the opportunity to review or to delete these communications before sending them, meaning covert access can be less privacy intrusive than real-time listening. However, this logic, while valid several years ago, has become less compelling as technology use and availability has changed.

Implementing a standard threshold for both content and stored communications warrants would remove the complexities inherent in the current interpretation of what is a serious offence, recognise the growing number of online offences and provide consistent protection for 'live' and 'stored' content. Consideration is also being given to reducing the number of agencies able to access communications information on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so.

Interception and stored communications warrants provide authority to receive the content of the communication and associated data. The concept of 'data' is not defined in the TIA Act but is generally understood to refer to information about a communication that is not the content or substance of a communication. Data is increasingly understood as falling into two categories: subscriber data, which provides information about a party to a communication such as name or billing address; and traffic data, which relates to how a communication passes across a network, such as the location from which the communication was made.

How and for what purposes an interception agency can intercept a communication depends on limited characteristics or features of the communication relating to the type of service or device used or the name of a person. Defining attributes by communicant, carrier-provided service or technology made sense in an era where carriers, device types and users were limited but is more complex in the current environment where the carrier or means of conveyance is not always readily apparent. This is both time-consuming and costly for agencies in terms of analysing unnecessary information and potentially invasive from a privacy perspective as the communications of innocent parties may be unduly affected. One way to address these concerns would be to introduce a simplified warrant regime that focuses on better targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest.

Streamlining and reducing complexity in the law

The use and disclosure of information obtained from exercising powers under the TIA Act is strictly regulated.

The Act prohibits the use and communication of information obtained under a warrant except for the purposes explicitly set out in the legislation. Information obtained under the TIA Act is subject to more rigorous legislative protections than other forms of information in an agency's possession. The provisions are detailed and complex in relation to record keeping, retention and destruction and can present a barrier to effective information sharing both within an agency and between agencies. This was not an issue when the Act was enacted and applied only to ASIO and the AFP, but with more agencies now defined as interception agencies and the national and transnational nature of many contemporary security and law enforcement investigations, effective co-operation within and between agencies is critical.

Simplifying the current information sharing provisions would support co-operative arrangements between agencies and consideration could be given to the ways in which information sharing amongst agencies could be facilitated.

Record keeping and accountability obligations require law enforcement agencies[27] to keep records relating to documents associated with the warrants issued and particulars relating to warrant applications (such as whether an application was granted or refused) and each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed. Agency heads must also report to the Attorney-General on the use and communication of intercepted information within three months of a warrant ceasing to be in effect. The Attorney-General's Department must prepare an annual statistical report about the use of powers under the TIA Act, which the Attorney-General tables in Parliament.

Different record keeping requirements apply to stored communications.

Oversight of law enforcement agencies' use of powers is split between the Commonwealth Ombudsman and equivalent State bodies in relation to interception activities. The Commonwealth Ombudsman inspects the records of both Commonwealth and State agencies in relation to stored communications. This split in responsibility contrasts with the *Surveillance Devices Act 2004*, where the Commonwealth Ombudsman inspects all agencies.

The requirements are aimed at ensuring that agencies keep appropriate records necessary to demonstrate that agencies are using their powers lawfully. However, many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate.

The current regime is focused on administrative content rather than recording the information needed to ensure that a particular agency's use of intrusive powers is proportional to the outcomes sought. The existing provisions take a one size fits all approach, resulting in a lack of flexibility for each agency to determine the best way to record and report on information having regard to individual practices, procedures and use of technology.

The same provisions also impede the Ombudsman's ability to report on possible contraventions and compliance issues by prescribing detailed and time limited procedures that need to be checked for administrative compliance, rather than giving the Ombudsman scope to determine better ways of assisting agencies to meet their requirements.

Consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes.

[27] The focus of the discussion about record keeping and accountability is on law enforcement agencies..

Modernising the cost sharing framework

Carriage and carriage service providers (C/CSPs), which are telecommunications industry participants subject to regulatory obligations under the TIA Act and the *Telecommunications Act 1997*, play an irreplaceable role in enabling agencies to access communications. Under the Telecommunications Act, C/CSPs have an obligation to provide such help to agencies as is 'reasonably necessary' for enforcing the criminal law and laws imposing pecuniary penalties, protecting the public revenue and safeguarding national security.

The TIA Act places an obligation on each C/CSP to have the capability to intercept communications and requires carriers and nominated carriage service providers to submit an annual interception capability plan outlining their strategy for complying with their obligation to intercept and to deliver communications to interception agencies. The obligation extends to maintaining the capability to intercept communications that are carried by a service that they provide and to deliver those communications to the requesting agency consistent with a warrant.

However, as networks have become more complicated and the types of services available have expanded, often beyond the C/CSPs' own networks, challenges have evolved in applying a general obligation. Consideration should be given towards introducing measures that implement more specific technical requirements to cater for a diverse and sophisticated telecommunications environment. This includes developing requirements around administrative needs such as the timeliness of cost sharing to agencies and the security measures to be applied to the handling of sensitive information relating to interception operations.

The capital cost of interception is shared between both industry and agencies. The cost of developing, installing and maintaining interception capability is borne by the C/CSP. The cost of developing, installing and maintaining delivery capability is borne by agencies. Costs have been split on that basis because industry is best placed to find efficiencies and to minimise costs. C/CSPs can recover the costs of providing day-to-day assistance to agencies on a no profit, no loss basis.

The TIA Act only covers C/CSPs, rather than the broad range of current telecommunications industry participants, consistent with the Act's focus on traditional services such as landline telephones. However, the exclusion of providers such as social networking providers and cloud computing providers creates potential vulnerabilities in the interception regime that are capable of being manipulated by criminals. Consideration should be given to extending the interception regime to such providers to remove uncertainty about the application of industry obligations in relation to agency requests and to better position Australia to meet domestic and international demands.

In reforming cost sharing, consideration must also be given to the current make-up of the telecommunications industry. The current requirements are predicated on the existence of one or few industry players and assume that all are resourced on a similar basis and have a similar customer base. This does not reflect industry practice which better suits a tiered model that supports comprehensive interception and delivery capability on the part of larger providers, a minimum interception and delivery capability on the part of medium providers and only reasonably necessary assistance for interception on the part of smaller providers.

A tiered model would also recognise that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant and less capacity to store and retain information about communications and customers. Requirements on industry to retain current information and to assist agencies to decrypt information would greatly enhance agencies' abilities to detect and disrupt criminal and other behaviours that threaten national wellbeing but should be implemented in a way that does not compromise business viability.

The merits of introducing a tiered model should be considered, including the role such an approach could play in defining industry obligations in relation to activities such as retaining data. A future framework for industry obligations would take into account not only regulatory best practice, but do so in a manner that minimises compliance costs for industry and maintains competitive neutrality. The Committee should also consider whether there are any broader competition impacts arising from the framework and its effect on prices.

Consideration should also be given to clarifying the role of the Australian Communications and Media Authority (ACMA) in regulating industry obligations under the interception regime. The ACMA has rarely used its powers to enforce compliance with the TIA Act because the only effective power available to it under the Act is court action. Court action is usually inappropriate or excessive in the circumstances and unhelpful from an agency perspective because it may publicly disclose that a particular C/CSP is not complying with its TIA Act obligations. The ACMA's role could be reinforced by expanding the range of regulatory options available and clarifying the standards with which industry must comply.

3. Next Steps

Access to communications content and data plays an important role in protecting the community against threats to security and serious criminal activity. It is vital that the legislation regulating the use of this investigative tool be kept up to date with developments in technology and the contemporary communications environment. Comprehensive reform of the current legislation is necessary, focusing particularly on the issues referred to the Committee by the Government and discussed in detail above.

CHAPTER THREE
TELECOMMUNICATIONS SECURITY SECTOR REFORM

1. Introduction

Australia's national security, economic prosperity and social wellbeing is increasingly reliant on the Internet and other information and communications technologies (ICT). Underpinning our use of these technologies is our telecommunications infrastructure. However, there are very real challenges to ensuring its security in the face of criminal and strategic threats. Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, accidental mis-configuration, external hacking and even trusted insiders.

Australian citizens, businesses and public entities rely on telecommunication carriers and carriage service providers (C/CSPs) to handle information and data on their networks, including customer information, securely. Telecommunications users, including businesses and consumers, reasonably expect that the information they store on, and transmit across, telecommunications networks is adequately protected from national security threats. Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians.

The Australian Government is considering whether telecommunications legislation, such as the *Telecommunications Act (1997)* (Telecommunications Act) and other relevant legislation should be amended to establish a risk based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure.

The desired outcomes of the proposed framework are that:

- government and industry have a productive partnership for managing national security risks to Australia's telecommunications infrastructure,
- security risks relating to Australia's telecommunications infrastructure are identified early, allowing normal business operations to proceed where there are no security concerns and facilitating expedient resolution of security concerns,
- security outcomes are achieved that give government, business and the public confidence in their use of telecommunications infrastructure for both routine and sensitive activities,

- the protection of information, including customer information and information about customers, contained on or transmitted across telecommunications networks is better assured, and
- compliance costs for industry are minimised.

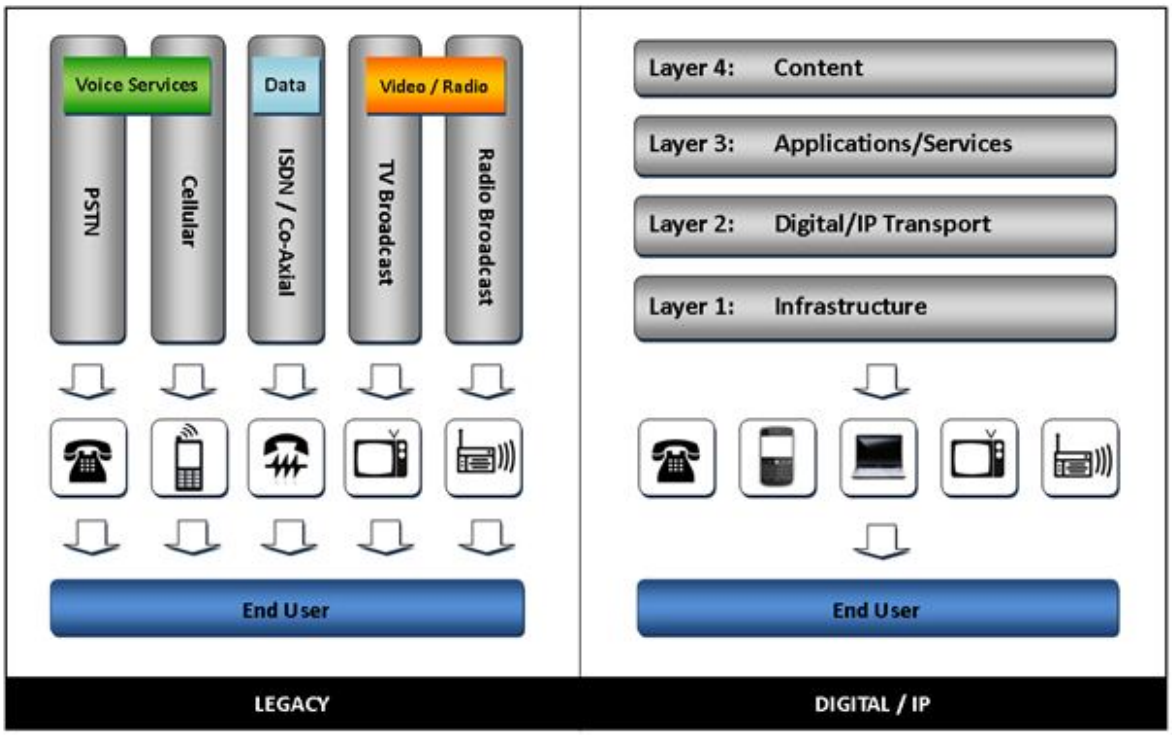
2. The context

While advances in technology and communications have resulted in unquestionable benefits to society and the economy, they have also introduced significant vulnerabilities, including the ability to disrupt, destroy, degrade or alter the functioning of our critical telecommunications infrastructure and the information held on it. A clear understanding of the current telecommunications environment is essential to identifying network vulnerabilities and managing them effectively. This includes the composition and operation of the telecommunications industry, national security risks, and the current regulatory environment.

2.1 Australia's telecommunications industry

Australia's telecommunications industry consists of a wide range of services and participants — an increasing number of which are based outside Australia. The telecommunications industry is a highly dynamic one, and C/CSPs usually operate network environments that have been significantly expanded and modified from their original specifications. In a broad sense, global telecommunications network architecture has evolved over the past 30 years from a 'siloed' services model to one of 'layered' convergence (figure 1). In Australia today, our telecommunications industry has evolved to reflect this shift, while the standardisation and mass-production of network equipment has also cut costs and opened up the range of suppliers with new entrants to the market gaining a stronger presence.

Figure 1: Convergence in network and service layers[28]



The National Broadband Network (NBN) rollout will further transform Australian telecommunications infrastructure, with changes to the telecommunications market's structure and functionality creating new opportunities for market participation. As such, Australia's telecommunications industry is increasingly diverse, with a range of overlapping and interconnected platforms and networks. The Australian Government recognises that C/CSPs operate in an increasingly competitive, commercial environment and that security is only one factor in procurement and investment decision-making. Although there are market incentives and customer expectations for network providers to ensure their infrastructure and services are secure, C/CSPs are working with incomplete information about the national security environment. There will always be information available to Government which is beyond industry's reach.

2.2 National security risks

The *ASIO Report to Parliament 2010-2011* states that espionage by foreign intelligence services is an enduring security threat to Australia, both conventional and new forms, such

[28] Australian Communications and Media Authority, 2011, Broken Concepts: The Australian Communications legislative landscape, p6 http://engage.acma.gov.au/wp-content/uploads/2011/08/ACMA_Broken-Concepts_Final_29Aug1.pdf

as cyber espionage. Our increasing reliance on communications technology to conduct the business of Government, commerce and our daily lives makes Australians more vulnerable to malicious attack. As such cyber security has emerged as a serious and widespread concern. [29] States, as well as disaffected individuals or groups, are able to use computer networks to view or siphon sensitive, private, or classified information for the purpose of, political, diplomatic or commercial advantage.

Individual records or files stored or transmitted on telecommunications networks may not be classified or particularly sensitive in and of themselves but, in aggregate, they can give foreign states and other malicious actors a range of intelligence insights not otherwise readily available. This threat extends to information vital to the effective day-to-day operation of critical national industries and infrastructure, including intellectual property and commercial intelligence.[30]

2.3 Current telecommunications regulatory environment

For the purposes of security, Australia's telecommunication industry is regulated primarily under two pieces of legislation — the *Telecommunications Act (1997)* administered by the Minister for Broadband, Communications and the Digital Economy and the *Telecommunications (Interception and Access) Act (1979)* (TIA Act) administered by the Attorney-General.

Section 581 of the Telecommunications Act provides the Attorney-General (in consultation with the Prime Minister and the Minister for Broadband, Communications and the Digital Economy) the power to give written direction to C/CSPs to cease supply of a carriage service if the use of that service is or would be prejudicial to security. It is recognised that such action, would impact on both businesses and consumers. Section 581 is non-specific, is not triggered by a specific set of circumstances and does not allow a practical graduated response to security risks. This sanction is a blunt instrument, and is not effective in encouraging C/CSPs to consider national security risks when making business decisions about the design of their networks.

Under section 202B of the TIA Act, C/CSPs are obliged to notify Government of planned changes to a telecommunications service or system where these changes may affect their capacity to comply with their obligations under the TIA Act. The TIA Act does not specifically address supply chain risks, hardware and software vulnerabilities or security risks to the confidentiality, integrity and availability of telecommunications infrastructure.

[29] ASIO, Director-General's speech at the Security in Government Conference, 7 July 2011

[30] ASIO, Director-General's speech at the Security in Government Conference, 7 July 2011

2.4 Analysis

Engagement between Government and the telecommunications industry about national security risks currently occurs on an informal basis, relying on co-operation between security agencies and C/CSPs in cases where security agencies become aware of potential risks. In most cases engagement between security agencies and C/CSPs has been constructive. However there is a lack of awareness of national security risks in business decisions by many C/CSPs, which means engagement often occurs late in the decision making process. A more defined framework for government's engagement with industry would minimise disruption and resource impacts for industry and government. It would also provide greater clarity for industry during a time of considerable structural change in the telecommunications industry.

Government is concerned that the telecommunications industry is not fully informed about national security risks and is therefore not equipped to respond adequately to these risks. As both businesses and consumers are also exposed to the consequences of potential security risks, there is a compelling case to act now. Australia is at a critical stage of telecommunications infrastructure development driven by the NBN's construction. Delaying action to make C/CSPs aware of managing national security risks will complicate long term management decisions made on the design and procurement of major telecommunications infrastructure, with potential negative impacts on national security.

Accordingly, Government has a responsibility to intervene in the market to educate and assist C/CSPs to maintain a minimum level of security for the purpose of protecting the data on their networks and, ultimately to ensure mechanisms are in place to support the integrity and security of Australia's national telecommunications infrastructure.

3. Proposed approach

One approach to address national security risks relating to telecommunications infrastructure may be achieved using a regulatory framework. Such an approach was developed earlier in 2012 for consultation with industry.

A regulatory approach could be achieved by making amendments to telecommunications legislation, such as the Telecommunications Act and other relevant legislation, such that C/CSPs protect their networks from unauthorised interference with the following elements:

1. an industry-wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure;

2. a requirement for C/CSPs to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure; and
3. powers of direction and a penalty regime to encourage compliance.

In designing a regulatory framework, the following principles are considered important elements of an effective regulatory system:

- be adaptable to a changing environment;
- be clear to industry;
- provide incentives for compliance;
- be reasonably equitable and competitively neutral; and
- not be resource-intensive for industry to comply or for government to administer.

The advantages of such a framework include that it could:

- focus on security outcomes rather than absolute technical requirements, making it adaptable to changes in technology and the telecommunications market,
- provide greater clarity, control and certainty for industry by focusing on self-governance and demonstration of compliance,
- can be applied equitably across the telecommunications sector, and
- provide a more effective incentive for industry to place greater emphasis on national security considerations in its business decisions.

The Government is aware that such a framework may have significant impacts for industry and agencies and welcomes input as it explores how such an approach could work in practice and what these impacts may be. Government would also welcome input on any broader competition impacts that the proposal may have on the telecommunications market and consumers more generally.

It should be noted that some classified national security information will only be able to be shared with companies that have entered into security agreements with Government, which have been negotiated on the basis of risk to the national interest.

3.1 Industry consultation

Preliminary targeted consultation with industry occurred in early 2012, during which C/CSPs demonstrated an understanding of the importance of protecting the confidentiality, integrity and availability of their networks.

Other points raised by industry included:

- the desire for a level playing field across the industry,
- a desire for clear guidance about Government's expectations and requirements for industry compliance,
- the need for certainty to enable C/CSPs to undertake business decisions with confidence, and
- flexibility for industry to explore and experiment with efficient and effective solutions for managing security risks.

During the consultation about a possible regulatory framework that originally included a notification obligation in place of the requirement to provide information to Government on request, industry expressed a preference for an approach that avoids the need for government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it. As a consequence an alternative regulatory framework designed with less focus on administrative processes and technical requirements, but greater emphasis on outcomes, has been developed for consideration.

3.2 Compliance framework

C/CSPs are obliged to protect the privacy of their customers' information; however there are many different ways that a C/CSP may be organised which will affect its ability to be able to confirm the security of its network and the information held on it. Where a C/CSP relies heavily on sub-contracted, outsourced or off-shored maintenance or services it will be more complicated to oversee the maintenance of security than a C/CSP that manages its network and information held on it in-house.

The industry consultation has led to consideration of whether a compliance framework, based on requiring C/CSPs to be able to demonstrate competent supervision and effective controls over their networks, may be a more effective approach. Such an approach would focus on the ability of a C/CSP to manage the security of its infrastructure and the information held on it. Information about a possible 'compliance framework' is provided below.

Competent supervision refers to the ability of a C/CSP to maintain technically proficient oversight (either in-house or through a trusted third party) of the operations of their network, and the location of data; awareness of, and authority over, parties with access to network infrastructure ;and a reasonable ability to detect security breaches or compromises.

Effective control refers to the ability of a C/CSP to maintain direct authority and / or contractual arrangements which ensure that its infrastructure and the information held on itis protected from unauthorised interference (which refers to network access). This might include arrangements to:

- cease contracts where there has been a security breach,
- direct contractors to carry out mitigation or remedial actions,
- oblige contractors to monitor and report breaches to the C/CSP, and
- repatriate information and network systems where unauthorised interference to a network has occurred.

Under such a compliance framework, Government would provide guidance to assist industry to understand and meet its obligation, and to inform C/CSPs how they can maintain competent supervision and effective control over their networks. Guidance would be tailored to C/CSP service types (for example internet service providers (ISP), backhaul service providers, and mobile virtual network operators) and distributed to C/CSPs prior to commencement of a framework.

The aim of such a regulatory framework would be to promote risk informed management of security in the telecommunications sector. This could be achieved by educating C/CSPs on national security risks and encouraging ongoing awareness and responsibility for network security, reducing the need for government intervention. Provision of general security advice, briefings and the development of guidance would be intended to be an ongoing, iterative process conducted in cooperation with industry, which would reflect evolving technologies and markets.

Under a regulatory framework Government would also disseminate information on specific security threats to affected C/CSPs on an as needs basis, including:

- targeted briefings (specific threat and risk information), and
- provision of specific mitigation information.

In order to monitor compliance with the obligations under a framework C/CSPs would be required upon request, to demonstrate compliance to Government. This could be done by compliance assessments and audits, based on a risk assessment to inform the level of engagement required. The level of engagement would be informed by factors such as:

- market share;
- customer base; and
- service offerings.

Government is giving consideration to the means by which it could be assured that industry had taken reasonable mitigations steps to address security risks. It would benefit from the Committee's advice on appropriate assurances mechanisms. These might include accreditation of industry for self-assessment purposes or a role for third parties in providing audit and assurance services. For example, in-depth compliance assessment and audits could focus on C/CSPs that security agencies consider are at greater risk of national security threats. Less intensive compliance assessment and audits would apply to selected C/CSPs from the broader pool of lower risk entities. This approach would monitor and evaluate industry-wide governance arrangements to ensure C/CSPs maintain competent supervision and effective control over their networks and facilities.

3.3 Directions and penalties

Government would seek to use advice and guidance to encourage risk informed management of security concerns. Where potential issues of concern are identified, the preferred approach would be to engage with the relevant C/CSPs to establish whether national security concerns can be co-operatively addressed. Where this is not possible, one way to proportionately address various levels and forms of non-compliance could be to provide a graduated suite of enforcement measures (including the power of direction). The availability of enforcement measures would provide industry with greater incentive to engage co-operatively with Government.

Under such an approach, in cases where engagement with C/CSPs proves to be ineffective, or a blatant disregard of security information jeopardises the Government's confidence in the security and integrity of Australia's telecommunications infrastructure, powers of direction could provide a proportionate means to achieve compliance. To safeguard such a power, it could require the Secretary of the Attorney General's Department, to seek the concurrence of the Director General of Security and the Secretary of the Department of Broadband, Communications and the Digital Economy, before directing a C/CSP to alter its business practices or undertake other actions considered necessary to protect national security interests. This would generally follow a period of more direct and intensive engagement with the C/CSP concerned.

Directions could involve targeted mitigation or remediation of security risks, including modifications to infrastructure, audit, and ongoing monitoring, with costs to be borne by the relevant C/CSP. Grounds for directing mitigation or alternative actions would ultimately be determined by security agencies, based on an assessment of risk following their engagement with a C/CSP. The powers of direction would serve as a means to support the existing powers in the Telecommunications Act relating to national interest matters.

To encourage C/CSPs' recognition and compliance with their security obligations under this regulatory framework, financial penalties are proposed. Financial penalties could be used in situations where, for example, a C/CSP fails to take reasonable action to protect its infrastructure and the information held on it. These penalties could be modelled on existing civil penalties contained in the Telecommunications Act.

As described earlier, the current provision under subsection 581(3) of the Telecommunications Act would remain available for the most serious security breaches. This enables the Attorney-General, in consultation with the Prime Minister and Minister for Broadband, Communications and the Digital Economy, to direct C/CSPs to not use or supply, or cease using or supplying, particular services where such use or supply would be prejudicial to security. As this direction only applies to a service as a whole, however; it cannot be used to restrict service use or supply to a particular organisation, group or person. As such, subsection 581(3) is considered an option of last resort, applicable in very limited circumstances.

Should a graduated suite of enforcement measures be made available under a regulatory framework, the following circumstances provide an illustration of where the Government may consider taking enforcement action:

- **where a breach has occurred**, for example a CSP's data is accessed and published, demonstrating a failure to protect its infrastructure and the information held on it from unauthorised interference;
- **where a C/CSP fails to provide reasonable assistance to Government to demonstrate compliance when requested;**
- **where there is failure by a C/CSP** to undertake mitigation activities that Government has determined are necessary to protect its infrastructure and the information held on it from unauthorised interference; or
- **where there is failure by a C/CSP to otherwise satisfactorily demonstrate it has competent supervision or effective control over its networks.**

The framework is intended to maximise cooperative engagement between C/CSPs and Government on matters of national security. Where such a relationship works effectively, there may be no need to invoke more formal directive powers. Administrative penalties or directions to C/CSPs would only be imposed where a risk has been assessed as significant and prior engagement has proved ineffective.

3.4 Transition arrangements

Should any legislative changes be agreed, this would require all C/CSPs to comply with the security obligations. In some instances this will require the application of mitigation measures to existing infrastructure. The security obligations would apply to existing and new infrastructure. Government recognises that it would need to work closely with industry to ensure that there is a reasonable transition period.

4. Next Steps

Government recognises that a regulatory framework would include a cost to industry, which may increase prices for consumers and it is working to understand these costs through targeted consultation. This work will be complemented by the Parliamentary Joint Committee on Intelligence and Security's consideration.

CHAPTER FOUR

AUSTRALIAN INTELLIGENCE COMMUNITY LEGISLATION REFORM

1. Introduction

It is the responsibility of Government to protect society against threats to our national security. The Government must be vigilant and take appropriate action to ensure that any threats to our national security do not materialise. Australian intelligence agencies have made a significant contribution to our safety by constant and careful assessment of possible threats.

However, the security environment is continually evolving and becoming increasingly diversified. Security legislation, and the ability of intelligence agencies to protect the security and safety of Australians and our democratic institutions, must also adapt and keep pace with these changes. To enable Australia's intelligence agencies to continue to protect national security, it is imperative that these agencies are appropriately equipped with the necessary statutory powers to uphold Australia's vital national security interests.

The Attorney-General's Department and Australian Intelligence Community agencies — including the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD), and the Defence Imagery and Geospatial Organisation (DIGO)—have identified a number of practical difficulties with the legislation governing the operation of these agencies, specifically the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act).

Addressing the problems outlined in this chapter of the Discussion Paper is necessary to maintain the intelligence gathering capabilities of the Australian intelligence agencies, ensuring they remain able to adeptly respond to emerging and enduring threats to security. Proposed reforms seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.

At the same time, it is important that legislation governing intelligence agencies continues to include appropriate checks and balances on the exercise of their powers. Ensuring these agencies remain accountable for their actions helps to maintain public confidence in and support for the crucial work of intelligence agencies. The proposed reforms seek to maintain a strong and accountable legislative regime under which intelligence agencies can respond effectively when threats to our community emerge.

This chapter of the Discussion Paper outlines the problems identified in the operation of both the ASIO and IS Acts and contains three sections relating to matters the Government wishes to progress, matters the Government is considering, and matters on which the Government expressly seeks the views of the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

2. Matters the Government wishes to progress

2.1 Modernise and streamline ASIO's warrant provisions

Division 2 of Part III of the ASIO Act contains a range of powers that ASIO can use under warrant in carrying out its statutory functions. The powers include search warrants, computer access warrants, listening and tracking device warrants, and the power to inspect postal or delivery service articles. Although there have been several amendments to each of these powers in the past, the amendments have been piecemeal and have not kept pace with technological advancements. To maintain effective intelligence gathering techniques and capabilities, these powers require modernising to provide a statutory framework which facilitates intelligence collection by the most technologically effective and efficient means.

References to 'computer' in section 25A

Computer access warrants under section 25A of the ASIO Act are limited to data stored on '*a computer*' ('computer' is defined to mean a computer, a computer system or part of a computer system). Therefore, if an individual has more than one computer which is not part of the same computer system, or data is stored on a computer network, more than one warrant may be necessary. For example, if there are multiple computers on a premises, and it is only discovered upon entering the premises for the purpose of executing a warrant that a particular computer is not connected to the computer system specified in the warrant, it would be necessary to seek another warrant (and enter the premises a second time) to access the data on that particular computer. This is inefficient and does not increase the level of accountability around the issue of warrants.

A possible solution to this issue could be to amend the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network.

Variation of a warrant

Currently, the ASIO Act does not specifically provide for a warrant to be varied if the circumstances justify such a variation. A new warrant is required in every instance where there is a significant change in circumstances. A variation provision may be appropriate to ensure sufficient operational flexibility while maintaining appropriate accountability.

Duration of warrants

All warrants under the ASIO Act currently last for a maximum of six months, except for a search warrant which must be executed within 90 days. A warrant enabling a search to take place within a six month period would provide operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors. Indeed, there have been instances where ASIO was unable to execute a search warrant within the 90 day limit for reasons beyond its control, and a new warrant would be required. .

To address this, the maximum duration of a search warrant could be increased from 90 days to six months, making it consistent with the other warrant powers in the ASIO Act.

Renewal of warrants

Certain threats to security can endure for many years, requiring a significant proportion of warrants issued under the ASIO Act to continue beyond the initial authorisation period. However, the current provisions in the ASIO Act do not enable a warrant to be extended.

In such circumstances, ASIO must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant change to either, and where the assessment of the intelligence case remains unchanged. A renewal process would provide appropriate oversight and accountability without requiring excessive administrative resources.

2.2 Modernise the ASIO Act employment provisions

Part V of the ASIO Act provides for the employment of ASIO officers and employees. These provisions do not align with the Australian Public Service (APS) framework as they were largely drafted over 30 years ago. Specific examples are discussed below.

Requirement to hold an "office"

Section 85 of the ASIO Act provides that the Director-General may determine the designation of officers in ASIO. Under subsection 85(1) of the ASIO Act, an officer must hold an 'office' that has been designated by the Director-General. With the exception of the Director-General, ASIO employees are no longer employed under the concept of the designation of 'office'. In practice, ASIO employees are employed under a concept of level. As it is no longer relevant, this section could be considered for deletion from the ASIO Act.

Descriptors of employment in the ASIO Act

The ASIO Act uses several descriptors to denote a person as an 'employee' of ASIO. These descriptors include 'officer,' 'employee' and 'staff' and are not separately defined in the ASIO Act. The use of the separate terms reflects the various amendments made to the ASIO

Act since 1979 but causes confusion as to whether differences between the terms are intended.

The use of the single term 'employee' throughout the ASIO Act would clarify and ensure consistency in the Act.

Special provisions relating to ASIO employees

Section 87 of the ASIO Act provides that the terms and conditions, under which ASIO employees were employed immediately before the date of commencement of the ASIO Act, continue to apply until they are varied by agreement. There are no longer any ASIO employees affected by section 87 and it could be considered for deletion from the Act.

Modernise the Director-General's powers in relation to employment terms and conditions

The Director-General's powers and responsibilities could be modernised so they are similar to those given to the CEO of a Commonwealth department or agency under the Public Service Act. This would ensure that, subject to guidelines issued by the Attorney under paragraph 8A(1)(b) of the ASIO Act, the Director-General has the power to engage employees on behalf of the Commonwealth, the rights, duties and powers of an employer and may determine terms and conditions of employment.

Proposed secondment arrangements

In order to access specialist skills and as part of arrangements whereby ASIO works closely with other agencies, ASIO often places staff of other agencies to work within ASIO, or agrees to its staff members working in other agencies. Legal complexities can arise in making such arrangements because of the specified scope of the functions and powers of ASIO and the other organisation involved.

If the ASIO Act were amended to expressly enable staff to be 'seconded' to and from ASIO and to clarify that, during the secondment, a seconded staff member carries out only the functions of the host organisation in accordance with any procedures or restrictions that apply under legislation to the host organisation, it would enhance ASIO's ability to engage with other agencies, and overcome administrative difficulties ASIO currently experiences in relation to existing secondment arrangements.

Such a secondment regime would operate independently from section 19A of the ASIO Act and section 13A of the IS Act. Section 19A enables ASIO to cooperate with and assist intelligence agencies, law enforcement agencies and prescribed Commonwealth and State authorities. An ASIO officer working in a multi agency task force operating under section 19A continues to carry out the functions of ASIO. Those functions would (as a consequence

of section 19A) include carrying out the functions of the other agencies involved in the task force. It is suggested that, unlike section 19A arrangements, these secondment arrangements would not be limited to intelligence, law enforcement and prescribed agencies.

2.3 Clarify the authority of the Defence Imagery and Geospatial Organisation

Minor amendments to DIGO's function under section 6B(e) of the IS Act would make some minor clarifications to ensure that DIGO has clear legislative support to undertake its geospatial and imagery related functions.

At present the IS Act enables DIGO under its subsection 6B(e) function to:

a. provide imagery and geospatial data to produce non-intelligence products for use by Commonwealth, State and Territory authorities, as well as for certain non government bodies and foreign governments approved by the Minister (paragraph 6B(e)(i))

b. provide technical assistance to the Australian Defence Force, Commonwealth, State and Territory agencies (as well as to certain approved non-government bodies and foreign governments approved by the Minister) in relation to the production and use of imagery and geospatial products, not being 'intelligence information' obtained for the purposes of subsections 6B(a), (b) or (c) (para. 6B(e)(ii)), and

c. provide assistance in relation to Commonwealth, State and Territory authorities (as well as for certain non-government bodies and foreign governments approved by the Minister) in relation to the performance of these authorities or bodies of emergency response functions (as defined by the IS Act).

DIGO's work under this function may therefore involve collecting imagery and other data in relation to locations inside and outside Australia, but what distinguishes its subsection 6B(e) function from DIGO's 'intelligence functions' under subsections 6B(a) to (d), is that the work is not done for the purpose of providing information about a particular person or entity. This does not mean that intelligence sources or capability are not utilised for the function, but rather DIGO's intent, or the activities which are undertaken for the purposes of this function, do not fall within the scope of 'intelligence information' purposes (as defined by the IS Act.)

It is proposed that, amending paragraph 6B(e)(ii) of the IS Act would clarify the activities that are included in the scope of this function. These amendments would seek to:

a. Clarify the scope of application of paragraph 6B(e)(ii) - The current wording of paragraph 6B(e)(ii) is; 'assistance in relation to the use of such imagery and products'. The inclusion of the word 'such' in this subsection has given rise to an unintended encumbrance, as it has the effect of linking this function to the preceding paragraph 6B(e)(i) function. The original intent of paragraph 6B(e)(ii) was to enable DIGO to provide expert technical assistance and advice on the production and use of all DIGO imagery and geospatial products, not only with respect to its 'non-intelligence information' activities and products covered by paragraph 6B(e)(i).

Paragraph 6B(e)(ii) could be amended to remove the word 'such', so as to avoid any doubt that DIGO is enabled to provide Commonwealth and State authorities, and other approved bodies, assistance in relation to the production and use of both non intelligence and intelligence imagery and geospatial products.

b. Include an express reference to specialised imagery and geospatial technologies - DIGO has an express function under paragraph 6B(e)(ii) to provide assistance in relation to the production and use of imagery and other geospatial products to Commonwealth, State and Territory authorities and bodies approved in writing by the Minister.

In line with this function (and implied under DIGO's 'communication' function in subsection 6B(d) for the purposes of subsections 6B(a) to (d)), DIGO assists Commonwealth, State and Territory authorities (as well certain non-government bodies and foreign governments as approved by the Minister) with the use and application of specialised imagery and geospatial technologies, including geospatial web-based services. However, this is not expressly provided for as a function of DIGO.

An express reference to this activity would avoid any doubt that DIGO is able to assist in this way and to ensure the prevention of any perceived gaps in DIGO's functions. These changes would further provide DIGO with the scope and flexibility to meet White Paper objectives, including the proposed acquisition of domestic satellite collection capability by Defence.

The proposed amendments do not change the original intended operation of section 6B of the IS Act. The existing safeguards in the IS Act would remain unaffected and in place. The suggested changes involve minor clarifications to provide more certainty and practical utility. By making the legislation clearer, it would be easier for the Inspector-General of Intelligence and Security to effectively review whether DIGO is operating within its powers, and ensure accountability is maintained.

3. Matters the Government is considering

3.1 Amend the ASIO Act to create an authorised intelligence operations scheme

ASIO's continued ability to collect useful and relevant intelligence on the most serious threats to the security of Australia and Australians, hinges on its capacity to covertly gain and maintain close access to highly sensitive information. This activity often involves engaging and associating closely with those who may be involved in criminal activity and therefore has the potential to expose an ASIO officer or human source to criminal or civil liability, in the course of their work.

With the enactment of broad overarching laws criminalising security related issues, many of those targets under investigation are involved in activities that breach the criminal law. Increasingly, those laws are capable of capturing the activities of persons who are associating covertly with targets, notwithstanding that their activities are for lawful intelligence collection purposes.

For example, under Part 5.3 of the Criminal Code, it is an offence to intentionally provide training to or receive training from a terrorist organisation where the person is reckless as to whether the organisation is a terrorist organisation. Therefore, if an ASIO officer or human source is tasked to collect covert intelligence in relation to a terrorist organisation, they may be open to criminal liability under the Criminal Code if, in the course of collecting the relevant intelligence, they receive training from that organisation.

An authorised intelligence operations scheme would significantly assist covert intelligence operations that require undercover ASIO officers or human sources to gain and maintain access to highly sensitive information concerning serious threats to Australia and its citizens. A scheme similar to the controlled operations scheme under the *Crimes Act 1914* could be developed to apply to ASIO officers and human sources operating under the ASIO Act, with appropriate modifications and safeguards that recognise the scheme would operate in the context of covert intelligence gathering investigations or operations.

Should an authorised intelligence operations regime be pursued, it will be critical that it achieves an appropriate balance between operational flexibility and appropriate oversight and accountability. Key features that may contribute to such could include:

- the Director-General of Security to issue authorised intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months)

- oversight and inspection by the Inspector-General of Intelligence and Security (IGIS), including notifying the IGIS once an authorised intelligence operation has been approved by the Director-General
- specifying conduct which cannot be authorised (eg, intentionally inducing a person to commit a criminal offence that the person would not otherwise have intended to commit and conduct that is likely to cause the death of or serious injury to a person or involves the commission of a sexual offence against any person), and
- independent review of the operation, effectiveness and implications of any such scheme, which could be conducted five years after the scheme's commencement.

3.2 Modernise and streamline ASIO's warrant provisions

Named person warrants

In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the different legislative requirements of the various warrant types, which is administratively burdensome.

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied.

Surveillance Devices – use of optical devices

Legislation governing ASIO's capabilities with respect to electronic surveillance has not been updated to align with legislation governing the use of electronic surveillance by law enforcement. ASIO's ability to use optical surveillance devices is tied to its ability to use listening devices. This is a relic of the time in which the ASIO Act was first drafted. Additionally, the administrative and procedural provisions governing the use of listening and tracking devices in the ASIO Act are not aligned with provisions governing the use of surveillance devices by law enforcement.

In practice, this acts as an impediment to effective cooperation and collaboration with law enforcement partner agencies. For example, the differences in scope and terminology between the ASIO Act and the Surveillance Devices Act limit actions which can be taken by each agency in working with partner agencies. Aligning the surveillance device provisions in the ASIO Act with the more modern Surveillance Devices Act could assist in overcoming these impediments to cooperation.

Authority for acts necessary to execute a computer access warrant

The increasingly complex nature of the global information technology environment and the use by some targets of sophisticated computer protection mechanisms can adversely impact ASIO's ability to execute a computer access warrant for the purpose of obtaining access to data relevant to security.

Subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be.

To address this, section 25A could be amended so that the prohibition does not apply to activity proportionate to what is necessary to execute the warrant.

Person searches

The ASIO Act currently contains the power to search a premises (section 25). Contained within this is the power to search a person who is *at or near* the premises where there are reasonable grounds to believe that the person has, on his or her person, records or other things relevant to the security matter (subsection 25(4A)).

Where ASIO assess that a particular person may be carrying items of relevance to security, a search warrant relating to a particular premises must be sought. It is only on or near the premises specified in the warrant that a person may be searched. However, it is not always feasible to execute a search warrant on a person of interest while they are *'at or near'* the premises specified in the warrant.

For example, some persons of interest employ counter-surveillance techniques such that predicting the likely timing and location at which a search would yield the desired intelligence dividend is not always possible. The existing limitation could be addressed by enabling ASIO to request a warrant to search a specified person rather than premises (subject to existing safeguards in subsections 25(4B) and 25AA) so that there would be sufficient operational flexibility while maintaining appropriate accountability via the warrant process.

Authorisation lists for warrants

Section 24 of the ASIO Act provides that the Director-General (or senior officer authorised in writing by the Director-General for the purposes of this section) may approve certain officers and employees to execute warrants issued under Division 2 of Part III of the ASIO Act.

The requirement to maintain a list of the individual names of each officer who may be involved in executing a warrant can create operational inefficiencies for ASIO. For example, sometimes the execution of a warrant takes place in unpredictable and volatile environments and ASIO needs to be able to quickly expand the list of authorised persons.

The problem could be overcome in large part if the Director-General could approve classes of people to execute a warrant. For example, the Director-General could authorise officers of a certain level within a particular Division of ASIO. Such persons at any one time would be readily ascertainable ensuring the level of accountability is not diminished, while improving operational efficiency.

3.3 Clarify ASIO's ability to cooperate with the private sector

Subsection 19(1) of the ASIO Act enables ASIO to cooperate with authorities of the Commonwealth, as well as Departments, police forces and authorities of the States, where it is necessary or conducive to the functions of ASIO. It is unclear whether section 19 could be read to imply that ASIO should not cooperate with organisations outside of government.

This concerns ASIO given the important role the private sector plays in Australia's national security, including by owning and operating a significant proportion of Australia's critical infrastructure. Furthermore, it is conducive to ASIO's functions to cooperate with the private sector. For example, ASIO's Business Liaison Unit (BLU), provides an interface between Australian business and the Australian Intelligence Community. The BLU provides intelligence backed reporting that can be used for risk management decision making. Such reports include reporting on the current security environment and threats to particular industry sectors.

It may be desirable to amend subsection 19(1) to avoid any doubt about ASIO's ability to cooperate with the private sector.

3.4 Amend the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act

Section 18 of the ASIO Act limits the circumstances in which a person can communicate information or intelligence acquired through their association with ASIO. In particular, information may only be passed to law enforcement agencies in relation to a 'serious crime' (defined as an offence punishable by imprisonment exceeding 12 months). Section 92, which makes it an offence for a person to publish the identity of an ASIO officer, is punishable by 12 months imprisonment. By virtue of section 18, ASIO is precluded from passing information about the possible commission of this offence to law enforcement agencies.

4. Matters on which the Government expressly seeks the views of the PJCIS

4.1 Modernise and streamline ASIO's warrant provisions

Use of third party computers and communications in transit

The ASIO Act recognises the importance of ensuring ASIO is able to access computers where necessary for the performance of its statutory functions and where approved by the Attorney-General.

However, advancements in technology have made it increasingly difficult for ASIO to execute its computer access warrants. Where a target is security conscious, innovative methods of achieving access to the target computer have to be employed. In the same way that access to a third party premises may be necessary to execute a search warrant, it may be necessary to use a communication that is in transit or use a third party computer for the purpose of executing a computer access warrant.

To overcome this problem, it may be appropriate to amend the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to lawfully access a target computer. Noting that using a communication in transit or a third party computer may have privacy implications, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme.

Incidental Entry

Sections 25 and 25A of the ASIO Act currently enable an officer, in the execution of a search or computer warrant, to do any thing that is reasonably incidental to the exercise of powers under that warrant. It is not clear whether this incidental power includes entry to a third party's premises for the purposes of executing the search or computer warrant. Additionally, it may be necessary to enter a third party premises for the purposes of installing a surveillance device. Clarification of the scope of the incidental power would assist ASIO in executing search and computer warrants.

Use of force

Subsections 25(7), 25A(5A), 26B(4) and 26C(4) relate to the use of force when exercising a power under a warrant and when entry into a premises is authorised under the warrant. The headings to each of those subsections suggest that the powers in those subsections are limited to entry to the target premises. The provisions relating to use of force are not limited in such a way. Technical amendments may therefore be necessary to correct this drafting anomaly.

Evidentiary Certificates

Currently, protecting information that reveals sensitivities about the identity of ASIO officers and capabilities used in the course of exercising special warrant powers relies on successful public interest immunity claims or, where available, orders obtained under the *National Security Information (Criminal and Civil Proceedings) Act 2004*. Unlike the *Telecommunications (Interception and Access Act) 1979* (TIA Act) and the *Surveillance Devices Act 2004* (SD Act), there is no consistent regime to protect ASIO information, capabilities and officer identities under the ASIO Act.

An evidentiary certificate regime could be introduced in the ASIO Act, similar to those which exist under the TIA and SD Acts, to provide a legislative basis for assisting ASIO to protect the identity of officers and sensitive capabilities involvied in the execution of warrant powers.

4.2 Amend the Intelligence Services Act 2001

Australia's foreign intelligence agencies, ASIS, DSD and DIGO, collect intelligence in accordance with requirements set by Government and operate under the IS Act. These agencies have identified problems arising out of the operation of the IS Act, which are considered below.

Ministerial Authorisations

The IS Act imposes strict controls on the ability of those agencies to produce intelligence on an Australian person. The Minister responsible for each Australian foreign intelligence agency is required to direct that the agency obtain authorisation from the Minister before undertaking an activity, or a series of activities, for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person.

Before giving an authorisation to produce intelligence on an Australian person, the responsible Minister must be satisfied under section 9(1) that:

- any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned, and
- there are satisfactory arrangements in place to ensure that
    - nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency, and
    - the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

According to section 9(1A)(a), before giving an authorisation to produce intelligence on an Australian person, the responsible Minister must be satisfied that the Australian person is, or is likely to be, involved in one or more of the following activities:

- activities that present a significant risk to a person's safety;
- acting for, or on behalf of, a foreign power;
- activities that are, or any likely to be, a threat to security (for this ground the Minister must also obtain the agreement of the Attorney-General);
- activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
- committing a serious crime by moving money, goods or people;
- committing a serious crime by using or transferring intellectual property;
- committing a serious crime by transmitting data or signals by means of guided and/or unguided electromagnetic energy; and
- activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law.

These activities do not specifically cover the situation where a person is or is likely to be involved in intelligence or counter-intelligence activities.

A new item could be added to the list in section 9(1A)(a) of the IS Act which would allow the Minister to give an authorisation if he or she is satisfied that the person is, or is likely to be, involved in intelligence or counter-intelligence activities. This would allow the Minister to issue an authorisation where the current grounds, for example, 'activities that present a significant risk to a person's safety,' are not available because the risk is to ASIS operations or is not specific to a person's safety.

In particular, this would assist ASIS to perform its existing function of conducting counter-intelligence activities under section 6(1)(c) of the IS Act and allow DSD and DIGO, at the request of ASIS and with approval from their Minister, to assist ASIS. In turn this would enable these agencies to protect their operations and those involved in them by allowing the agencies to produce intelligence on a person who the Minister is satisfied is, or is likely to be, involved in intelligence or counter-intelligence activities. This activity may detect the interference of a foreign power, in which case ASIO would normally become involved in assessing any threat to security.

It is imperative that Australia's intelligence agencies are appropriately equipped to protect Australia's vital national security interests. This includes the ability for Australia's foreign intelligence and security services to interact and work seamlessly together.

In March 2011, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* made amendments to the ASIO Act and the IS Act to enable Australia's intelligence agencies to more closely cooperate and assist one another in the performance of each other's functions. Specifically, section 13A of the IS Act was introduced to facilitate greater cooperation in multi-agency teams, such as under the Counter Terrorism Control Centre, which is hosted by ASIO, and enable agencies to harness resources in support of key national security priorities.

However, there are differences in the legislative regimes which apply to ASIS, DSD and DIGO under the IS Act and to ASIO under the ASIO Act when they produce intelligence on Australian persons. In part these differences reflect the different nature and functions of the IS Act agencies and ASIO. When the agencies are cooperating and assisting ASIO in the performance of ASIO's functions, these differences have led to situations being identified where ASIO is able to undertake an activity for the purposes of its functions but an agency subject to the IS Act may not be able to fully cooperate with and assist it.

To better meet the intention of enabling Australia's intelligence agencies to cooperate and assist each other in the performance of each other's functions to protect Australia and Australians, section 13A of the IS Act could be amended. For example, section 13A could be amended to enable the Minister responsible for an IS Act agency to authorise specified activities where the agency is cooperating with ASIO in the performance of an ASIO function. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required. This change would create greater consistency between the ministerial approval regime that applies to the IS Act agencies and the approval regime which applies to ASIO.

The proposal is principally intended for ASIS and ASIO cooperation relating to the capabilities, intentions and activities of people or organisations outside Australia. Given existing Defence agencies' functions and capabilities, and the nature of the activities to which the proposal is sought to address, it is unlikely that Defence would utilise the proposed change.

The existing safeguards in the IS Act could apply to the proposed section 13A authorisation. These include the requirement for all ministerial authorisations to be provided to the IGIS who oversees the legality and propriety of the operations of the intelligence agencies. Additionally, the communication and retention of intelligence collected under the ministerial authorisation would be subject to the Privacy Rules.

The proposed changes to section 13A could also operate in a limited set of circumstances:

- A ministerial authorisation under the proposed changes to section 13A would usually only be issued for a discrete activity for a specified purpose where ASIS is cooperating with ASIO in connection with the performance of its functions. This category of ministerial authorisation will not be able to be issued to ASIS, DSD and DIGO to assist another IS Act agency, or a prescribed Commonwealth authority, or a State authority.
- A ministerial authorisation under section 13A will not replace the need to obtain a warrant where a warrant would currently be required under the ASIO Act or the TIA Act.
- Renewal could be sought, but where a ministerial authorisation under a section 9(1A) ground could be sought, further ministerial authorisation would need to be sought under sections 8 and 9 of the IS Act rather than as a renewal of the section 13A authorisation.

ASIS co-operation on self-defence and weapons training

ASIS operates in a number of very dangerous locations overseas. In recognition of this, the IS Act was amended in 2004 to enable ASIS staff members and agents to receive training in the use of weapons and self-defence techniques, subject to a number of important safeguards (schedule 2).

However, under this regime, ASIS is only permitted to provide training in the use of weapons to ASIS staff members and agents. The IS Act does not currently enable ASIS staff members to participate in joint training in the use of weapons with persons cooperating with ASIS, even though ASIS staff members are authorized to use weapons to protect such persons. At a practical level, the current inconsistency restricts joint training activities because ASIS trainers cannot run training that includes individuals who are not ASIS staff members.

Such cooperation would not enable ASIO officers to carry weapons or receive training from ASIS in the use of weapons. Co-operation on weapons training would be limited to Commonwealth, State and Territory bodies that have, under some other law, a right to carry weapons in the course of their duties. This will cover training with law enforcement and military personnel.

Such cooperation would enable ASIS to cooperate with a limited number of approved overseas authorities in the delivery of training in self defence and weapons. Such cooperation could be limited to authorities approved by the Foreign Minister under section

13(1A) of the IS Act. Such an approval requires the Foreign Minister to first consult with the Prime Minister and Attorney-General.

5. Next Steps

This Chapter has discussed the Australian Intelligence Community legislative reform aspect of the package of reform proposals referred to the PJCIS for inquiry and consultation. The Government recognises that some of the reforms are controversial and may attract significant media interest. To avoid public misunderstanding as to the nature of these reforms, it is imperative that the PJCIS take into account a wide range of views on the proposals from public stakeholders and government agencies. This will ensure that any measures brought forward to enhance the intelligence gathering capabilities of our intelligence agencies continue to be subject to appropriate checks and balances on these powers.

CONCLUSION

The preceding chapters of this Discussion Paper have elaborated on the complex international security environment in which our intelligence and law enforcement agencies operate. Ideas for telecommunications interception reform (Chapter 2), telecommunications sector security reform (Chapter 3) and Australian intelligence community reform (Chapter 4) seek to equip these agencies with the capability to meet today's emerging national security challenges.

In light of the issues discussed, the Government seeks the views of the PJCIS on the package of ideas. This Discussion Paper will prove useful as a basis for stakeholder consultation. A number of key industry representatives and Government agencies will seek to provide their views on the proposals to the PJCIS.

GLOSSARY OF KEY TERMS

The ACMA – The Australian Communications and Media Authority

Ancillary service providers

Telecommunications industry participants who are not carriers or carriage service providers.

Anonymous pre-paid services

A mobile phone or other communications service where credit is purchased in advance of the service being used. In circumstances where the pre-paid service can be obtained without providing personal details, or by providing false details, the service is an 'anonymous' pre-paid service.

ASIO – Australian Security Intelligence Organisation

ASIS – Australian Secret Intelligence Service

ASIO Act – *Australian Security Intelligence Organisation Act 1979*

Calling cards

Otherwise known as telephone cards, are pre-paid cards which allow payment for telephone services. Calling cards are typically intended for use by travellers.

Carriage service providers

A CSP is an entity that supplies a carriage service to the public using a telecommunications network unit. CSPs can include organisations that resell time on a carrier network for phone calls, provide access to the internet (Internet Service Providers) or provide telephone services over the internet (VoIP service providers).

Carrier

A carrier is an owner of a telecommunications network unit that is used to supply carriage services to the public. Carrier licences are granted by the Australian Communications and Media Authority (ACMA) under section 56 of the Telecommunications Act.

Ciphers

A method of transforming text in order to conceal its meaning.

Communications Packets

A formatted unit of data which comprises a communication passing over a packet-switched network.

Content

The substance of a communication, for example the subject line and body of an e-mail or what is said during a phone call

Data

Information about a communication that is not the content or substance of a communication

Data retention

The storage of telecommunications data for prescribed periods of time.

Data set

The specific set of data that would be required to be retained under a data retention regime

Decryption

The act of decoding of encrypted information into a meaningful form.

DIGO – Defence Imagery and Geospatial Organisation

DSD – Defence Services Directorate

Encryption

The encoding of data so that it cannot be decoded without appropriate software or hardware, so as to prevent authorised access.

e-payment

Payment for buying and selling goods or services offered through the Internet, or more broadly, any type of electronic funds transfer.

Gigabytes

For digital information or computer storage a gigabyte represents 1 billion bytes.

GPS - The Global Positioning System

A space-based satellite navigation system that provides location and time information anywhere on Earth

ICT – Information and communications technology

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Identifiers to communications

Information such as a phone number or email address, linking the target of an interception warrant to the service or device to be intercepted.

Industry Participant

Any member of the telecommunications industry, including carriers, carriage service providers and ancillary service providers.

Inter-carrier roaming agreements

An agreement between carriers to ensure that wireless devices remain connected to the network despite changing locations.

IS Act – *Intelligence Services Act 2001*

ISP – Internet Service Provider

An ISP is any entity that provides access to the Internet.

IP – Internet Protocol

A standard protocol for transmission of data from source to destinations in packet switched communications networks and interconnected systems of such networks.

Megabits

For digital information or computer storage a megabit represents 1 million bits.

NBN – National Broadband Network

The National Broadband Network is a next-generation broadband network. The network comprises three technologies – optic fibre, fixed wireless and next-generation satellite – and will provide more reliable, high-speed broadband access to all Australians.

Penalty Units

An amount of money used to determine a pecuniary penalty – currently $110.

Propriety data formats

A file or communication format that is the intellectual property of an individual or organisation.

PSTN - Public switched telephone network

The network of the world's public circuit-switched telephone networks. It consists of telephone lines, fibre optic cables, microwave transmission links, mobile networks, communications satellites, and undersea telephone cables, all inter-connected by switching centres, allowing any telephone in the world to communicate with any other.

Resold services

A service which is provided by a wholesaler and resold to customers via another telecommunications industry participant.

SD Act – *Surveillance Devices Act 2004*

Serious offence

An offence that carries a penalty of at least 7 years' imprisonment or a range of offences for which it is already recognised that general community standards would expect interception to be available, such as child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks

Smartphone Technology

Mobile phones built with mobile computing capabilities.

Stored communications

Communications which are no longer passing over the telecommunications system, held on carrier equipment and cannot be accessed on the equipment by a person who is not a party to the communication without the assistance of an employee of the carrier.

Stored communications Warrant

A warrant authorising access to stored communications.

Suborning

Bribery or procurement of a person to commit some unlawful or wrongful act.

Subscriber data

Information about a subscriber to a communications service, such as name or billing address.

Telecommunications System

A system over which telecommunications are transmitted. It comprises of three primary units, a transmitter, a transmission medium and a receiver.

Terabytes

For digital information or computer storage a gigabyte represents 1 trillion bytes.

Terminal device

A device which the end user interacts with that terminates one end of a communication, such as a phone or computer.

TI – telecommunications interception

TIA Act – *Telecommunications (Interception and Access) Act 1979*

Traffic data – information relating to how a communication passes across a network, such as the time, duration or location from which the communication was made.

Transactional data

Data describing an event, including when it occurred.

TSSR – Telecommunications Sector Security Reform

TSSR refers to the proposed regulatory framework being explored by Australian Government, which aims to manage and mitigate national security risks associated with telecommunications infrastructure.

VoIP – Voice over Internet Protocol

A technology that allows real-time voice conversations over the Internet.