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

**May 2012**

# 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.*

# 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 (the Committee) 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*, and
   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 element of the National Security Legislation referral to the Attorney-General on a date to be determined].*

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.

***Modernising lawful access to communications and associated communications data***

*Telecommunications (Interception and Access) Act 1979*

1. Reforming the lawful access to communications regime. This would include examination of:
    a. reducing the number of agencies eligible to access communications information
    b. the standardisation of warrant tests and thresholds
    c. expanding the basis of interception activities
2. Streamlining and reducing complexity in the lawful access to communications regime. This would include examination of:
    a. simplifying the information sharing provisions that allow agencies to cooperate
    b. removing legislative duplication
    c. creating a single warrant with multiple TI powers
3. Modernising the TIA Act's cost sharing framework. This would include examination of:
    a. aligning industry interception assistance with industry regulatory policy
    b. clarifying ACMA's regulatory and enforcement role
    c. implementing detailed requirements for industry interception obligations
    d. extending the regulatory regime to ancilliary service provides not currently covered by legislation
    e. implementing a three-tiered industry participation model
    f. establishing an offence for failure to assist in the decryption of communications
    g. instituting industry response timelines
    h. tailoring 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
4. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the 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

***Mitigating security and resilience risks to Australia's communications networks***

*Telecommunications Act 1997*

1. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would include examination of :

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

   b. 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

***Enhancing the operational capacity of Australian intelligence community agencies***

*Australian Security Intelligence Organisation Act 1979*

1. Modernising and streamlining ASIO's warrant provisions. This would include examination of:

   a. enabling warrants to be varied by the Attorney-General, simplifying the renewal of warrants process and extending duration of search warrants from 90 days to 6 months (for consistency with the duration of other warrants under the ASIO Act)

   b. establishing a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a singl target insread of requesting multiple warrants against a single target

   c. establishing classes of persons able to execute warrants

   d. introducing an evidentiary certificate regime

   e. aligning surveillance device provisions with the *Surveillance Devices Act 2004*

f. updating the definition of 'computer' in section 25A of the ASIO Act

g. enabling the disruption of a target computer for the purposes of a computer access warrant

h. permitting use of third party computers and communications in transit to access a target computer under a computer access warrant

i. enabling person searches to be undertaken independently of a premises search

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

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

2. Modernising employment provisions in the ASIO Act. This would include examination of:

   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

3. Examining a possible new authorised intelligence operations scheme under the ASIO Act, providing ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.

4. Making other amendments to the ASIO Act to clarify and address matters that have arisen with existing provisions. This would include examination of:

   a. clarifying ASIO's ability to cooperate with the private sector

   b. 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

*Intelligence Services Act 2001*

1. Amending the Intelligence Services Act 2001 to clarify and address matters that have arisen with existing provisions. This would include examination of:

    a. clarifying the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies

    b. adding 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

    c. enabling 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)

    d. enabling 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.

---

[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

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:

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

## 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.

[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.

## 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 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 organisations 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.

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

[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.

## 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 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]

---

[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.

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.

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.

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

### *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 Providers (VOIP), 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]

---

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

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

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

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 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

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

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

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

[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

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]

***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

[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

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

### *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

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

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.

### *Modernising the cost sharing framework*

Carriage and carriage service providers (C/CSP's), 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.

### *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.

## 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.