Submission No 218

Inquiry into potential reforms of National Security Legislation

Organisation: **Attorney-General's Department**

Attorney-General's Department Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into Potential Reforms of National Security Legislation – Terms of Reference relating to reform of the interception regime

The primary function of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) is to protect the privacy of the communications of people who use Australian telecommunications networks. Without this legislation any government agency, person or business could covertly access the communications of any person at any time for any purpose.

The TIA Act is an important part of Australia's privacy framework ensuring that covert access to communications can occur only in circumstances designed to benefit and to protect the safety and wellbeing of Australians. Details about the current legislative framework are provided at **Attachment A**.

Historically, the TIA Act and its 1960 predecessor protect the privacy of communications by prohibiting interception except as allowed under the conditions specified in the Act. The concepts underpinning those conditions replicate many of the communication methods that existed in the 1960 Act, the nature of the telecommunications sector at the time and the focus of law enforcement and national security agencies as existed in 1979. While the fundamental concepts remain valid and continue to be consistent with broader privacy principles, many of those assumptions are now being tested by the rapid change in the contemporary communications environment.

As the combustion engine, air travel, space flight and the advent of the computer marked the first seventy years in the last century so the last five years have been dominated by the revolution in communications technology. Social media, smart phones and the rapid growth of the online world are still in their early days but have already caused a monumental shift in the way people communicate and transact with each other. These new media are also changing the ways in which organised criminals and people who want to do harm to Australia operate.

The technological and cultural implications of this revolution are generating significant challenges for law enforcement and national security agencies in accessing communications to maintain existing and future investigative capabilities. While agencies continue to adapt their capabilities within the constraints of the current legal framework this has not completely addressed the impact of rapid change in the telecommunications environment.

Access to communications and telecommunications data have provided critical evidence in Australia's most high profile terrorist and other criminal prosecutions providing an effective and efficient method of obtaining critical evidence and intelligence. This access is increasingly important as it is predominately the only avenue for agencies to investigate and to respond to serious and online crime and the emerging risks of cyber-threats.

However, access to this information is being undermined by new technologies and the dynamics of the evolving communications environment. The TIA Act was enacted in an era with a Commonwealth Government-owned telecommunications monopoly (Telecom) and simple landline technology. Over the last 15 years, with deregulation, the telecommunications environment has evolved to encompass new industry structures and business models and entirely new technologies. These changes are presenting an increasing number of challenges to the effective operation of the TIA Act and are impeding the ability of

agencies to respond with proportionate, effective investigative capabilities to undertake the roles these agencies have been entrusted to perform.

Since 1994 six major reviews have dealt with telecommunications interception, the last in 2009, all of which have resulted in ad-hoc amendments to the interception regime. However, no holistic reform has occurred since the TIA Act came into effect in 1979.

The package of proposals provided to the PJCIS for its consideration and review provide a way forward for building a contemporary interception regime that better protects privacy interests by expressly recognising the changing communications landscape and which maintains the effectiveness of interception as an investigative tool now and into the future.

The Telecommunications Interception Regime

The TIA Act has continued to work for so long because it is drafted in terms that do not refer to particular types of technology. Instead of terms like 'telephone' the Act refers to a 'telecommunication system' and 'telecommunications service,' concepts which over the years have been able to adapt and apply to a landline, a mobile device and an internet service.

Underpinning the TIA Act are various assumptions about how communications are made which reflect the communications environment that existed in 1979 when the Act was made. The TIAAct assumes that:

a) Communications to be intercepted are easily identified
b) A stream of traffic to be intercepted can be isolated from the rest of the communications passing over the network
c) Carriers and carriage service providers (C/CSPs) that is telecommunications companies and internet service providers control the traffic passing over their networks
d) C/CSPs are the only entities which control public telecommunications networks
e) Intercepted communications are easily interpreted or understood
f) There are reliable sources of associated telecommunications data that link people to communications, and
g) A one size approach to industry obligations is appropriate.

Technological changes in the types and availability of communications devices, changes in the make-up of the telecommunications industry and cultural changes in the way Australians communicate as discussed at pages 17-22 of the Attorney-General's Department discussion paper 'Equipping Australia Against Emerging and Evolving Threats' (extracted at **Attachment B**), mean that these assumptions no longer underpin the majority of modern communications.

As a result, the TIA Act has been subject to 20 pieces of amending legislation since 3 May 2006. These amendments have retained the currency of the Act but on a reactive basis that clarifies the application of the regime to a new or emerging issue.

The magnitude of current and anticipated change to the telecommunications landscape means it is now timely to consider whether the privacy needs of Australians and the investigative needs of law enforcement and national security agencies are best served through continuous ad-hoc change or whether the time is right to put in place a new interception framework that squarely focuses on the contemporary communications environment. The Department considers that holistic reform would establish a new foundation for the interception regime

that enables users and participants, as well as the broader Australian community to understand their powers, rights and obligations.

The core changes to the telecommunications access regime relate to:

1. Clarifying the application of interception powers
2. Recognising current telecommunications industry participants and modernising obligations
3. Mandatory data retention, and
4. Safeguards to protect the privacy of communications.

1. Clarifying the application of interception powers

The TIA Act provides for several separate warrants for law enforcement agencies to access content, including warrants relating to accessing real-time content, and one warrant to access '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.

The stored communications regime allows 'enforcement agencies' to access the content and associated data of a communication held by a carrier. The category is broad as any agency with functions that include administering a law imposing a pecuniary penalty, or a law relating to the protection of the public revenue is an 'enforcement agency'.

How and for what purposes an interception agency can intercept a communication currently depends on limited characteristics or features of the communication relating to the type of service or device used or the name of a person. Warrants are effectively available for either a service or a device. Carriers initiate interception based on the identifiers included in the warrant. For instance, if a suspect is using a smart phone connected to a carrier called The Friendly Telephone Company, then The Friendly Telephone Company can intercept against the phone number it has given the suspect or it can intercept all communications to and from the handset number when the handset is connected to its network.

Defining the limits of a warrant by carrier-provided service or technology made sense in an era where carriers and devices were limited but is more complex in the current environment where new services and technologies are being rapidly created and implemented, the carrier or means of conveyance is not always clear and where there is no clear relationship between a service and the end user. In the current framework intercepting a persons communications may require the issue of a large number of warrants due to the diverse range of services and devices available to a person of interest. In 1979, arguably it would have been possible to have a maximum of two warrants to cover all communications available to the person of interest. **Attachment C** is a diagramatic example of the services and devices available in 1979 compared to 2010.

Other factors, such as portability of phone numbers and the number of providers in Australia mean that communications between two or more parties can involve a number of routes and companies. The volume of information collected is both time-consuming and costly for agencies in terms of analysing irrelevant material 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. Such characteristics could go beyond phone numbers and device identifiers to include more specific details that better target and isolate the communications of interest. The very nature of a person's communications, such as the regularity of calls to a particular number can be a better identifier than the type of device used to make the call, enabling communications of interest to be described in greater detail. The imperative to only target communications of interest is growing with data volumes increasing rapidly and consumer demand for high speed broadband expected to drive up data flows for many years to come.

Hypothetical scenarios can illustrate shortcomings with the current regime and the merits of targeting characteristics. Consider the following:

> A rural property is rented by a drug gang that houses a drug lab built in the basement. The lab is protected at all times by members of the gang who live in the house. The property is not connected to any communications services. The rural location makes covert human surveillance difficult. Investigators have ascertained that the gang's head cook visits the house every Thursday afternoon and also has possession of multiple mobile phones and SIM Cards from a small phone company. The drug cook makes the drugs and then uses a disposable phone and pre-paid SIM to call the head of the gang in Sydney. The investigating agency does not know who the head of the gang is. The drug cook, after making the call, destroys the SIM and the phone.

Under current legislation, the police cannot intercept the drug cook's calls because they cannot identify the service before it is used. The service is never re-used. Utilising characteristics of the communications, (such as Thursday afternoons, from the phone tower closest to the clan-lab, using the relevant provider, and to Sydney) would allow the police to obtain a warrant to intercept communications made by the drug cook.

Warrants relating to accessing real-time content are traditionally limited to investigating an offence that carries a penalty of at least seven years imprisonment: a 'serious offence' as defined in section 5D of the TIA Act. Section 5D is an exhaustive list which includes offences by reference to other Commonwealth legislation (such as an offence against Part 10.7 of the *Criminal Code Act 1995*) or of a certain type (such as murder) or involving certain conduct (such as trafficking in prescribed substances) all of which generally require at least seven years imprisonment.

In Australia, agencies cannot get a person's real-time content without an independently issued warrant. Warrants are only issued if an agency can convince an issuing authority that a 'serious offence' is being investigated.

The Department considers that these requirements should not change: access to real-time content should continue to be subject to an independently issued warrant for the investigation of a serious offence.

Over time though, numerous amendments to the TIA Act to reflect new crime types and changes in law enforcement priorities have made section 5D of the Act lengthy, complex and less clear as to when interception is available. The different categories within section 5D of the TIA Act mean that some of the offences for which interception is available are relatively low, while other offences with significant penalties fall outside the definition. For example, recklessly dealing with proceeds of crime worth less than $1000 is a serious offence, however there is no obvious part of section 5D of the TIA Act which allows interception for the

investigation of rape, rather, warrants for such investigations are argued on the basis that the conduct being investigated involves a serious risk of causing harm to a person.

The Department is concerned that the growing complexity of section 5D of the TIA Act is inefficient in terms of police resources needed to clarify the application of the provision in specific circumstances and, more importantly, potentially privacy invasive in its lack of clarity about how and when interception can be used.

By contrast, a stored communications warrant can be issued for the investigation of an offence carrying a penalty of at least three years' 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 unlike a telephone call, people can review or delete their communications before sending them, meaning covert access is less privacy intrusive than real-time listening. However, this logic has become less compelling as technology use and availability has changed. People now often use messages rather than voice as their primary form of communication making it difficult to draw a meaningful privacy distinction between stored and live communications.

The Department considers that the interception regime would offer greater privacy protection if the distinction between stored and live warrants was removed and if a standard threshold for both content and stored communications warrants was introduced. Reliance on the higher seven year penalty threshold has not proved successful in limiting the application of interception powers. On the other hand the three year stored communications threshold underestimates the value of non-voice communications in the contemporary communications environment. A threshold in between these two would recognise the growing importance of non-voice communications and enable interception to be used as a tool in investigating a number of serious crimes that currently fall outside the TIA Act.

A single warrant, and clarification of the concept of serious offence, would greatly enhance the capacity of the interception regime to ensure that interception is only available in defined circumstances.

2. Recognising current telecommunications industry participants and modernising obligations

Industry participants

The current legislation places obligations on 'carriers' and 'carriage service providers' as defined by the *Telecommunications Act 1997* (the Telecommunications Act):

- Section 7 of the Telecommunications Act states that 'carrier' means the holder of a carrier licence. Carriers are owners of telecommunications infrastructure who have been issued with a licence by the Australian Communications and Media Authority (ACMA).

- The Telecommunications Act defines 'carriage service provider' in section 87 as a person who supplies a carriage service to the public using a network owned by a carrier, a line connecting outside Australia or a satellite facility. Section 7 of the Telecommunications Act defines 'carriage service' as a service for carrying communications by means of guided and/or unguided electromagnetic energy.

In reality, the telecommunications industry has evolved and developed into a much wider range of relevant participants. There are many more products and services now on offer than traditional voice and email services, including those from offshore providers. New products can be developed quickly and can rapidly spread throughout the marketplace. Traditional services provided by carriers such as landline voice services are increasingly being replaced by newer services such as internet telephony.

The development of the National Broadband Network (NBN) allows a broad range of content service providers to utilise this optical fibre network to retail services to the general community. It will be necessary to ensure that relevant communications can still be accessed from the retail service providers, since the NBN will not hold such communications, as the NBN will have no end-user customers.

There are a large range of newer industry participants to the telecommunications industry that provide infrastructure, services, equipment, software, hardware or applications that provide or facilitate communications using a telecommunications system. These participants are the 'owners' of information that may be of assistance to national security and law enforcement agencies in undertaking their functions effectively, including:

- electronic messaging service providers, which includes webmail providers, instant messaging providers, text messaging providers, and similar providers social networking providers
- internet telephony (voice over Internet Protocol - VoIP) providers
- encryption service providers
- cloud computing providers
- data storage and cache providers
- authentication, authorisation and accounting (AAA) providers
- public network access providers
- tele-hosting providers
- internet assigned name and domain name registrars, and
- content service providers.

The Department considers that industry obligations should apply to all such industry participants so as to ensure both existing and emerging products and services are covered, and are not outside law enforcement's powers. This will ensure that people cannot 'technology shop' to avoid detection. Such obligations would provide a level playing field across providers ensuring that Australian providers are competitive and innovative in the provision of services.

Encryption

Encryption is becoming widespread in information and communications technology. Criminals and terrorists are increasingly using encryption to avoid detection, investigation and prosecution causing difficulties for agencies to access clear, intelligible communications in their operations.

Encryption can be difficult to manage. It may not always be the case that a person who uses or creates encryption is able to provide assistance with decryption. Often an applications provider, organisation or individual provides encryption services, rather than a carrier. Criminal organisations and terrorists can obtain these services or even create and use their own encryption solutions.

Section 3LA of the *Crimes Act 1914* (the Crimes Act) sets out provisions concerning decryption regarding information obtained under search warrants; however this does not extend to communications intercepted pursuant to a warrant under the TIA Act.

In summary, section 3LA of the Crimes Act allows a police officer to apply to a magistrate for a warrant to require a person to provide in accessible form (i.e. in decrypted form) data held on a computer or data storage device, where the computer or data storage device had been seized under a warrant. A warrant may be applied to the person under investigation, an owner of the device, an employee of the owner, a relevant contractor, a person who has used the device, or a systems administrator. There is a penalty of up to two years imprisonment for failing to comply with an order.

A consistent approach to that contained in the Crimes Act would ensure that information lawfully accessed for national security or law enforcement purposes under the TIA Act was intelligible.

3. Mandatory Data Retention

Need for a data retention model

A key challenge is retaining the capacity of agencies to access telecommunications data. Telecommunications data is information about communications, such as the time of the communication, the name and billing address of the party to a communication. It does not include the content of a communication itself. A potential data retention regime would not include the retention of the content of communications.

Traditionally generated and retained by industry for business and taxation purposes, such as billing, tax returns and resolving customer complaints and available to law enforcement and national security agencies under the interception regime, evolving technologies and business models mean that telecommunications data is no longer being consistently retained.

The capacity to lawfully access telecommunications data held by C/CSPs is a vital tool for agencies to investigate and solve crime and to protect national security. There are no operational risks associated with access to telecommunications data, it incurs minimal costs and raises fewer privacy concerns because of the non-content nature of the information than other covert investigative methods.

Crime continues to occur and targets of interest, now more than ever, are utilising the wide range of telecommunications services available to them to communicate, coordinate, manage and commit serious crimes. The availability of encrypted services is also impacting on the capacity of agencies to use content making telecommunications data a highly valuable investigative tool. Indeed industry has acknowledged that the value of telecommunications data, depending on the circumstances, can be as important, or more important, than the content of communications.

However, despite the increasing reliance on telecommunications data, industry has confirmed that there will be changes (reductions) in the type of telecommunications data that is created and the timeframes it is retained into the future. Industry has indicated that this is a natural evolution as a result of advances in technology and business models.

Currently, upon receipt of a valid authorisation under the TIA Act for access to telecommunications data the C/CSP gives what they retain to the requesting agency. What information is retained, and therefore is available to agencies, depends on the C/CSP. As discussed above, C/CSPs may keep relevant telecommunications data for business purposes such as taxation and billing for up to seven years, however, there is no uniformity about what telecommunications data is kept and the length of time it is retained.

For example, cell tower telecommunications data which allows agencies to establish a geographic location of a mobile device with a high degree of accuracy is currently retained by industry participants for different timeframes between eight weeks to three years.

Such information, which is consistent with the location information printed on a mobile phone bill, is critical in finding lost, missing or abducted persons, including dementia patients and persons with a disability who become separated from a carer, and individuals or groups lost in the bush, as well as gathering information about a suspect. The information also plays a key role in exonerating people early in an investigation by ruling them out based on their proximity to the scene of a crime.

The evolution of technologies and business models is also impacting on the availability of telecommunications data.

For example, the telecommunications sector is migrating from traditional Public Switched Telephone Networks to internet protocol (IP) based networks. Internet based service providers tend to charge on the quantity of data used rather than on a per call basis and therefore may not have a business requirement to retain billing information on who called whom, when and where and the time of each call.

Despite these challenges, the evolution to IP-based networks also means that for some types of communications there can be substantially more telecommunications data generated by the telecommunications systems and it can be more valuable than the content of those communications that may be encrypted.

Anecdotal reporting from agencies is that increasingly requests for telecommunications data are not being met as carriers do not retain the particular telecommunications data requested. Unfulfilled requests waste agency resources, inhibit the making of requests, and can lead to investigations being stalled or abandoned with crimes going unsolved.

Some suggestions have been made that a data preservation model would be a viable alternative to data retention.

Data preservation involves a C/CSP preserving specific telecommunications data identified by an agency that it has available on its network in relation to a relevant investigation or intelligence gathering activity on notification by an agency. Given the current authority under the TIA Act for agencies to access telecommunications data from a C/CSP when it has been identified as being relevant to a specific investigation or intelligence gathering activity, agencies already have the ability to access telecommunications data that the C/CSP has on hand at the time of the request or that comes into existence into the future, negating the need for data preservation.

Without an obligation for C/CSPs to retain telecommunications data for a set period of time, agencies ability to trace communications in retrospect will diminish in line with C/CSP's business models to base customer billing on data volumes rather than communications events.

Agency access to telecommunications data

Currently, access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an 'enforcement agency' to authorise a C/CSP to disclose telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. There are separate provisions enabling access for national security purposes.

An enforcement agency is broadly defined as all interception agencies as well as a body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. In practice, the range of agencies that are enforcement agencies and which authorise the disclosure of telecommunications data is very broad and includes Shire Councils, Government Departments and Agencies such as Centrelink and bodies as the Royal Society for the Prevention of Cruelty to Animals (RSPCA) (which plays a role in investigating assaults and other criminal acts against animals).

While data plays a critical role in law enforcement the value of that data in terms of the information it can provide increasingly goes beyond the traditional information similar to an entry in the White Pages. The diverse range of agencies that can access data and the degree of data generated by the IP world in particular suggests that consideration could be given to distinguishing between data types so as to allow certain agencies access to less descriptive forms of data while restricting access to more detailed data types.

International Comparison

European Union

The European Union (EU) has had a mandatory data retention regime in place since March 2006 to retain telecommunications data for use by law enforcement and security agencies. The European Directive has been transposed into domestic law by 26 EU member states, although it has been subject to some challenges by privacy and consumer groups. The constitutional courts of three countries (Germany, Romania, and the Czech Republic) annulled the domestic legislation based on a finding that the domestic laws transposing the obligations exceeded the requirements set out in the Directive and were therefore disproportionate and unconstitutional. The Czech Republic and Romania are currently considering how to re-transpose the Directive into domestic legislation.

The European Directive included a requirement for an evaluation of the application of the Directive and its impact which was to be prepared by the European Commission. This report was published on 18 April 2011. The report concluded that overall, the evaluation had demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU. The evaluation highlighted the lack of harmonisation in transposition of the directive in areas such as purpose limitation, retention periods and reimbursement of costs for industry (which is outside the scope of the Directive).

In light of these conclusions, the European Commission has announced that it intends to propose amendments to the Directive, but is yet to announce the detail of those amendments. Any amendments are not expected to be implemented until after the implementation of

amendments to the related EU Directive 2002/58 on Privacy and Electronic Communications (concerning the processing of personal data and the protection of privacy in the electronic communications sector).

United States of America

In May 2011, the United States of America introduced the Protecting Children from Internet Pornographers Act of 2011 which requires electronic communications providers to retain, for a period of at least 12 months, all records or other information relating to the identity of a user of a computer network. The Act is yet to be passed.

4. Safeguards to protect the privacy of communications

The TIA Act contains numerous restrictions on the access, use and disclosure of communications lawfully obtained by agencies as well as comprehensive record keeping and reporting requirements with independent oversight. Broadly the prescriptive nature of the exceptions reflects the intrusive nature of the collection of the information as well as public expectations about how this information may be dealt with.

The Department considers that these important checks, balances and limitations on the operation of the regime should remain a part of the underlying principles of the telecommunications access regime. However, barriers to the effective and efficient use of information obtained should be removed to reflect changes in the way agencies conduct their investigations. This would include ensuring that specialist agencies such as the Australian Securities and Investments Commission and the Australian Customs and Border Protection Service are not impeded in their investigations.

It is also important that these principles are evaluated and assessed in line with any modernisation to the legislation to ensure that they reflect the changing nature of technologies and the privacy needs of contemporary communications users.

Additionally, a privacy focused objects clause that clearly articulates this important objective will complement the numerous safeguards built into the operation of the TIA Act by underpinning the ongoing interpretation of obligations under the Act.

Conclusion

The utility of access to telecommunications is clearly demonstrated in its ability to provide critical evidence and intelligence in terrorist and other criminal prosecutions. There is a risk that if nothing is done to reform the TIA Act agencies will be unable to arrest the serious decline of this important investigative capability and the effectiveness of national security and law enforcement agencies across the nation will be seriously impacted. The techniques and tools available to counter most of these challenges are available but are incompatible with the existing assumptions on which the legislative framework is drafted. If such tools are not permitted to be adopted, agencies must rely on legacy techniques which will in time fail them and seriously compromise the ability of agencies to continue to successfully fulfil the roles that they have been entrusted to undertake.

Attachment A

CURRENT LEGISLATION FRAMEWORK

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 *Telecommunications (Interception and Access) Act 1979* (TIA Act). The TIA Act contains provisions for covert access to communications and telecommunications data by law enforcement and national security agencies (interception agencies) and other Commonwealth, State and Territory enforcement agencies.

The TIA Act enables the real-time interception of communications, such as listening to a phone call as it occurs, and access to past communications stored on a carrier or carriage service provider's (C/CSP's) network, such as emails, under a warrant in defined circumstances. The TIA Act also allows access to telecommunications data (information about a communication, such as the time and duration of a phone call or subscriber details) for defined purposes as an exception to the general prohibition to accessing information protected under the *Telecommunications Act 1997* (Telecommunications Act).

Interception (Part 2-2 and Part 2-5 of the TIA Act)

A warrant is issued to the agency by an independent authority and allows for the interception of communications passing over a telecommunications system. Warrants identify either a telecommunications service or a named person. The warrant is served on the C/CSP that carries the communications service that is the target of the interception or that are sent or received by a device, such as an identified mobile phone.

An independent authority is, in the case of a law enforcement agency, a Judge or nominated Administrative Appeals Tribunal member. In the case of the Australian Security Intelligence Organisation (ASIO), the warrants are issue by the Attorney-General. The independent authority may issue the warrant if satisfied from the facts outlined in the affidavit that:

- there are reasonable ground for suspecting that the person is using or is likely to use the service
- that information obtained under interception would be likely to assist the investigation of a serious offence in which the person is involved
- and having regard to:
    - the privacy of any persons likely to be interfered with by interception
    - the gravity of the conduct being investigated, and
    - the extent to which other methods of investigating the offence have been exhausted or would prejudice the investigation.

In Australia, 17 agencies can apply for telecommunications interception warrants. ASIO may obtain a warrant with respect to their legislative functions relating to security. The AFP and State/Territory police agencies also have access to these powers for the investigation of serious offences. The remaining eight agencies are a mix of agencies whose functions relate to police

integrity, anti-corruption and serious and organised crime who may also access tehse powers for the investigation of serious offences.

Whilst traditionally limited to an offence that carries a penalty of at least seven years' imprisonment which also involves certain listed conduct, there are exceptions to this general threshold to include specific offences for which interception warrants may be sought (for example, child exploitation offences).

The warrant authorises interception of communications and the associated telecommunications data that travel over the network by way of a telecommunications service operated by C/CSP for the period the warrant remains in force.

Stored communications (Part 3-2 and Part 3-3 of the TIA Act)

A stored communication is a communication that is accessed after it has finishing travelling over the communications network. Stored communications are accessed retrospectively (i.e. after they have been sent) and are accessed from the carrier as the communications are stored on the C/CSP's network or equipment. Examples of the types of communications that may become stored and would be provided under a stored communications warrant include emails, SMSs and voicemail messages. The stored communications regime allows enforcement agencies to access communications content and the associated telecommunications data (i.e. the data associated with the content) held by a carrier under a stored communications warrant.

A stored communications warrant may only be issued for the investigation of an offence carrying a penalty of at least three years' imprisonment or a fine of 180 penalty units.

A stored communications warrant may only be sought by an agency which falls within the definition of 'enforcement agency'. An enforcement agency is defined in the TIA Act as a criminal law-enforcement agency, a civil penalty enforcement agency or public revenue agency. This includes all the bodies mentioned as interception agencies and eligible authorities for the purposes of telecommunications interception warrants, a broad range of other agencies and bodies. In practice, because only enforcement agencies that are investigating offences which meet the legislated threshold (three years or 180 penalty units) may seek an interception warrants, only regulatory bodies such as the Australian Customs and Border Protection Service, the Australian Securities and Investments Commission and the Australian Competition and Consumer Commission have sought warrants for access to stored communications.

Telecommunications data (Part 4-1 of the TIA Act)

Telecommunications data is information about communications, such as the time of the communication but is not the content of the communication itself. Subscriber data is a type of telecommunications data, and provides information about a party to the communication, such as name or billing address. Traffic data is another type of telecommunications data and relates to how the individual communications pass across a network on which the communication was made.

Telecommunications data may only be disclosed to an 'enforcement agency'. This is the same range of agencies who may seek access to stored communications. Telecommunications data may be sought where it is for the performance by ASIO of its functions, the enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty, the protection of the public revenue or the location of a person who is the subject of a missing person report. A broad range of agencies have enforcement functions and currently access telecommunications data including the Australian

Fisheries Management Authority who investigate illegal activities by domestic and foreign fishing boats and may impose pecuniary penalties and the Royal Society for the Prevention of Cruelty to Animals who investigate and prosecute serious animal cruelty.

The regime also enables a criminal law-enforcement agency as defined by the TIA Act (all interception agencies as well as the Australian Customs and Border Protection Service) to authorise the disclosure of prospective telecommunications data. Prospective telecommunications data is data that is yet to come into existence, this includes location based telecommunications data that is provided from the C/CSPs network infrastructure. Access to prospective telecommunications data has a higher threshold than historical data and can only be authorised for the investigation of an offence against a law that is punishable by imprisonment for at least three years. Prospective telecommunications data is generally provided to the agency in near real-time for the duration of the authorisation (45 days for law enforcement agencies and 90 days for ASIO).

Dealing with information (Part 2-6, Part 3-4 and Division 6 of Part 4-1 of the TIA Act).

The use and disclosure of information obtained from exercising powers under the TIA Act is strictly regulated. There is a general prohibition on dealing with:

- interception warrant information,
- or information that has been obtained through interception, and
- information that has been obtained pursuant to a stored communications warrant.

The TIA Act provides exceptions to these general prohibitions which detail when TIA Act information may be used and communicated, for what purposes, in what type of proceeding and to whom. These exceptions vary depending on what type of information and which agency.

Intercepted information is generally allowed to be dealt with for the purpose of the investigation of the offence for which the information was sought. The intercepted information may also be used in connection with the investigation of any offence with a maximum of at least three years imprisonment. The TIA Act lists which agencies an interception agency may pass intercepted information to and for what purposes. For example, the Australian Federal Police may share intercepted information with the Australian Securities and Investments Commission (ASIC) when jointly undertaking and investigation but the TIA Act prohibits ASIC from using this information for its own purposes, even if one such purpose was the investigation of an offence with an imprisonment period of at least three years.

Stored communications information is generally allowed to be dealt with for the purpose of the investigation of the offence for which the information was sought. The stored communications information may also be used in connection with the investigation of an offence with a maximum of at least 12 months imprisonment or a fine or pecuniary penalty of 60 penalty units (individual) or 300 penalty units (non-individual).

The thresholds for secondary dealing with telecommunications data are the same as the thresholds for access to the information that is; for the performance of ASIO of its functions, the enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty, for the protection of the public revenue and for the for the purposes of finding the missing person.

Information obtained by way of the TIA Act is subject to more rigorous legislative protections than other forms of information in an agency's possession.

Oversight (Part 2-7, Part 2-8, Part 3-5, and Part 3-6)

Interception agencies are required to keep records in relation to interception which include the documents associated with warrants issued, particulars relating to warrant applications (such as whether an application was granted or refused), and particulars relating to each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed.

There are also record keeping requirements relating to agencies that access stored communications warrant information. For accessed telecommunications data, the head of an agency is required to keep a copy of each authorisation made for a period of three years.

In relation to interception, the head of each agency must provide a report to the Attorney-General regarding the use and communication of information obtained under an interception warrant within three months of a warrant ceasing to be in force. The TIA Act also requires the Managing Director of a C/CSP to prepare a similar report in relation to each interception warrant they action.

The Attorney-General's Department is required to prepare an annual statistical report, which the Attorney-General tables in Parliament.

Law enforcement agencies' use of powers under the TIA Act is oversighted by independent agencies such as the Commonwealth Ombudsman, State Ombudsman or equivalent body as provided by the relevant state or territory legislation. The results of inspections are required to be reported annually to the Attorney-General, although the Commonwealth Ombudsman may report to the Attorney-General at any time about inspections.

The Inspector General of Intelligence and Security inspects records kept by ASIO and the results of inspections are included in ASIO's annual report to the Parliamentary Joint Committee on Intelligence and Security.

Industry obligations (Chapter 5)

The TIA Act places an obligation on each C/CSP to have the capability for interception. The TIA Act does not specify standards for this capability. However, carriers and nominated carriage service providers must annually submit an interception capability plan which outlines their strategy for compliance with the obligation to intercept and deliver communications to the relevant agencies. This plan is submitted to the Communications Access-Coordinator within the Attorney-General's Department.

The TIA Act requires that industry has the capability to intercept communications that are carried by a service that they provide and to deliver those intercepted communications to the agency.

Industry has obligations to provide such help as is 'reasonably necessary' for the purposes of enforcing the criminal law or law imposing pecuniary penalties, protecting the public revenue and safeguarding national security. This obligation is contained within the *Telecommunications Act 1997* and includes the provision of interception services, giving effect to a stored communications warrant, providing information about intercepted or stored communications received under a warrant and giving effect to telecommunications data authorisations.

The Australian Media and Communications Authority have a role in regulating industry obligations under the TIA Act.

Cost allocation principles (Part 5-6)

The TIA Act outlines the principles for cost allocation for interception. The 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 initially borne by the C/CSPs, but these costs are recovered from agencies. Delivery points are the demarcation point/s between interception capability and delivery.

The Telecommunications Act provides that C/CSP can recover the costs of providing reasonably necessary assistance in actioning a stored communications warrant or an authorisation for access to telecommunications data. The C/CSP may neither profit from nor bear the costs of providing assistance.

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.

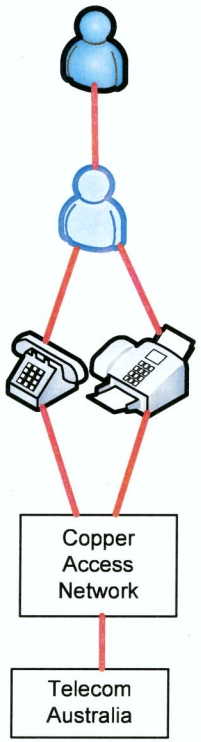
Four main areas have been identified as requiring review:

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

1979

Direct, unambiguous relationships between user identity, numbering plan and service provider.

Simple, unintelligent terminal devices with limited pre-defined functionality – 'device identity' unimportant to network operation.



User (Target)

Identity

Devices

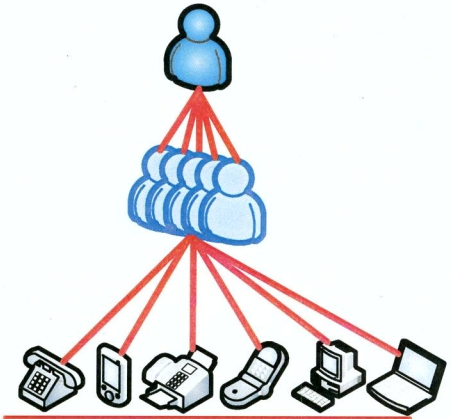
Network Access

Network Providers

Internet Access Providers

Application Service Providers

2010



Multiple identities possible. Anonymity common. No direct, unambiguous relationships between user identity, numbering plan and service provider.

Many terminal devices now programmable (by providers and users) and with a device identifier. 'Device identity' known to network.

Many Relationships Possible

Cable and FO Access Networks, including NBN	Copper Access Network	WiFi Access Networks	Wireless Access Networks	Satellite Access Networks

Many Relationships Possible

Telstra	Singtel Optus	VHA	Transact	Primus	AAPT	Many Others...

Many Relationships Possible

Big Pond	OptusNet	Internode	iiNet	iPrimus	AAPT	Many Others...

No Limit to Relationships

MSN	Google	Yahoo!	Facebook	Twitter	eBay	Many Others...