Submission No 163

Inquiry into potential reforms of National Security Legislation

Organisation: Australian Federal Police

AFP submission to

Parliamentary Joint Committee on Intelligence & Security Inquiry into National Security Legislation

Introduction

Since 1979 the Australian Federal Police (AFP) has been protecting Australia and Australian interests. In addition to providing a traditional law enforcement role focused on disrupting criminal activities and the arrest of criminals, the AFP also has responsibilities in meeting the government's national security and intelligence priorities. As a progressive, multi-faceted law enforcement agency the AFP is committed to utilising cutting-edge skills and expertise to combat serious and organised crime and other threats to our national security.

Telecommunications interception and access to telecommunications data are essential tools for law enforcement, however, the *Telecommunications (Interception and Access) Act 1979* (TIA Act) was drafted at a time when telecommunications was based on a copper wire and landline network. Substantial and far reaching changes to the telecommunications industry, communications technology, community and criminal use of telecommunications all mean that the modern environment is now vastly different to that which the TIA Act was based. This has driven numerous amendments to the TIA Act in recent years and as the rate of technological change continues to accelerate the legislation is increasingly struggling to keep pace. The AFP believes holistic reform is needed to adequately address current and future communications technology, in order to avoid further degradation of existing capability, whilst still maintaining appropriate accountability to the Parliament and through Parliament accountability to the community we serve.

The AFP welcomes the opportunity to make a submission to this Inquiry. This submission addresses the TIA Act terms of reference only. This submission first sets out relevant background on the current operation of the TIA Act and the AFP's institutional arrangements to support the accountable use of interception powers. The second part of the submission addresses the Committee's terms of reference in relation to telecommunications interception and non-content telecommunications data disclosure. The AFP has included a series of scenarios based on cases that demonstrate the limitations of the current TIA Act and the need for reform.

Part 1

<u>What the TIA Act authorises the AFP to do now</u>

The TIA Act has two primary objectives:

(i) to protect the privacy of individuals who use the Australian telecommunications system, and

(ii) to specify the limited circumstances in which it is lawful to intercept, and access communications or authorise the disclosure of non-content telecommunications data.

The AFP supports the maintenance of these two key purposes.

TIA Act currently achieves these outcomes by:

- prohibiting any listening to or recording of the content of communications unless under warrant for the investigation of a serious offence
- prohibiting access to the content of stored communications unless under warrant for the investigation of a serious offence or contravention
- establishing processes to enable limited disclosure of telecommunications data to assist in the enforcement of the criminal law, laws imposing criminal penalties and laws aimed at protecting public revenue.

The AFP is one of a limited number of interception agencies to whom warrants can be issued in connection with the investigation of serious offences. In addition to setting out the circumstances under which such warrants may be obtained and how they must be executed, the TIA Act also defines the infrastructure via which interception can be enabled. It contains significant administrative, reporting and oversight measures designed with the intention of ensuring the accountable use of lawful interception, stored communications access and authorised release of non-content communications data.

Telecommunications Interception

Telecommunications are intercepted on the basis of traditional identifiers primarily being particular services provided by a Carrier or Carriage Service Provider (C/CSP) or identifiers attached to a particular physical device. Part 2-5 of the TIA Act provides for the issue of warrants to agencies to assist with the investigation of a serious offence. The range of serious offence is defined in section 5D and includes the following types of offences:

- murder, kidnapping and equivalent offences
- serious drug offences
- terrorism offences
- offences punishable by at least 7 years imprisonment that involve conduct such as:
    - Risk of loss of a person life, serious personal injury, serious property damage endangering personal safety serious arson bribery or corruption, and tax evasion, fraud, loss of revenue to the Commonwealth;
    - offences relating to people smuggling, slavery sexual servitude, deceptive recruiting and trafficking in persons;
    - sexual offences against children and offences involving child pornography;
    - money laundering offences, cybercrime offences, serious cartel offences; and
    - offences involving organised crime.

The types of Telecommunications interception warrants available are:

- telecommunications service interception warrants, which authorise the interception of a traditional telecommunications service such as a phone number linked to person suspected of involvement in a serious offence. In limited circumstances these warrants may allow interception of identified telecommunications services of a person not under investigation but known to communicate with the person suspected of involvement in a serious offence (section 46) ;

- named person warrant which authorise the interception of a number of telecommunications services provided by a C/CSP and used by a person or the telecommunications devices used by a person, where that person is suspected of involvement in a serious offence (section 46A); and

- warrants which authorise entry on to premises where it would be impracticable to intercept communications without the use of equipment installed on those premises (section 48)

Access to stored communications

In addition to lawfully warranted interception Part 3.3 of the TIA Act regulates enforcement agencies access to stored communications. Stored communications are those that either have ceased, or have not commenced, passing over a telecommunications system, and can only be accessed by the parties to the communication and the C/CSP who owns the system on which they are stored. The TIA Act protects this information by making it an offence for a person to access a stored communication without the knowledge of the sender or the intended recipient of the communication.

An exception from this prohibition exists which allows warrants to be obtained for covert access to stored communications by declared enforcement or national security agencies, including the AFP, when the specific thresholds set out in the TIA Act are met.

A stored communications warrant may only be issued in respect to an investigation of a serious offence or a 'serious contravention' which is defined by the TIA Act as a:

- an offence punishable by a maximum period of imprisonment of at least three years imprisonment; or

- an offence with an equivalent monetary penalty.

Disclosure of non-content telecommunications data

In line with other records available for disclosure to Law Enforcement such as electoral role records and those relating births death and marriage the TIA Act also includes provisions allowing for the lawful disclosure by C/CSP's of historical and prospective non-content telecommunications data. Disclosure is only

permitted where it is determined to be reasonably necessary for agencies' investigations.

The lawful release of non-content telecommunications data is a vital investigative tool for law enforcement. Given that it reveals only data about communications rather than any content it raises fewer privacy concerns than the use of lawful interception.

While non-content telecommunications data has not been defined in the TIA Act, it is taken to mean anything that does not include the content or substance of a communication. It can include:

- subscriber information;
- telephone numbers of the parties involved in a communication;
- the date, time and duration of a communication;
- location-based information, and
- Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication.

Historical non content communications data is information which existed before an authorisation for disclosure was received. Its disclosure may be authorised by an enforcement agency only when it is considered reasonably necessary:

- for the enforcement of a criminal law;
- a law imposing a pecuniary penalty, or
- for the protection of the public revenue.

Prospective non-content communications data is that which comes into existence during the period the authorisation is in force. The disclosure must only be authorised when it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years.

Each request by an AFP case officer for disclosure of non-content telecommunications data requires the relevant criminal offence to be specified for consideration and authorisation by an officer at or above the rank of Superintendent..

The AFP retains records relating to all requests for non-content telecommunications data.

How does the AFP undertake interceptions

The Telecommunications Interception Division (TID) is located in the AFP's High Tech Crime Operations (HTCO) portfolio and its function is to support investigations by providing monitoring, record-keeping and report services in accordance with the TIA Act.

The TID is responsible for the management of lawfully intercepted information and the provision of evidentiary packages in support of AFP prosecutions. It also facilitates inspections by the Commonwealth Ombudsman's Office to ensure best practise and legislative compliance in all aspects of the regime.

HTCO has invested in building an enhanced technical surveillance system (ETS) used by the TID which integrates surveillance device and telecommunications interception material into a secure platform to best utilise information in support of AFP investigations. This initiative ensures effective and secure use of intercepted information in a controlled environment.

How does the AFP use the powers under the TIA Act?

The TIA Act requires record keeping and reporting on every warrant issued to the AFP as well as the submission of an annual report relating to agency use of the powers under the TIA Act. The report covers a wide range of themes including:

- the number of applications for warrants made and the number of warrants issued to an interception agency, and
- the number of applications made by an agency for disclosure of non-content telecommunications data.

In the year ending 30 June 2012 the AFP made 541 applications for interception warrants and 22 900 requests for historical non-content telecommunications data.

When considering these figures and the use of TIA Act powers by the AFP, it is important to take into account the shape of the Australian telecommunications and internet industries and the widespread use of their services by the community.

The ACMA Communications Report for 2010-2011 reveals that in Australia at the end of June 2011 there were:

- 29.28 million mobile services ;
- 10.55 million fixed line telephone services, and
- 10.9 million Internet subscribers.

In addition to this, rapid change in the sector is in progress:

- Industry is moving from circuit switched systems for telecommunication to IP based infrastructure resulting in for example increased use of Voice over Internet Protocol (VOIP) services;
- Australian consumers are increasingly accessing multiple technologies and services to communicate, with 58% of adults who use a fixed line service also using a mobile phone, a VoIP service and the Internet;

- Increasing globalisation of services means that Australians may be using telecommunication provides that are based overseas for Internet or VoIP services, and

- growing numbers of services such as Blackberry's and Smartphone applications are default encrypted.

Part 2 Why does the TIA Act need to be reformed?

Extensive change has taken place in the Australian and international telecommunications sectors since 1979. The technological developments of just the last 10 years have revolutionised communications and the pace of the changes continues to gather momentum. The rapid and expanding uptake of new ways and means of communicating denotes a transition to a new operating environment where the traditional concepts of C/CSP as the primary facilitators of communication no longer apply.

Law enforcement interception capabilities are increasingly being undermined by these fundamental changes in the telecommunications industry and communications technologies. The changes go to the very heart of how communications travel over the telecommunications network and challenge the assumptions on which the TIA Act and agency capabilities are based.

Targets of interest continue to utilise a wider range of the telecommunications services available, to communicate, and to coordinate, manage and commit crimes. This proliferation of new services and ways to communicate is impacting on agencies' opportunities to utilise telecommunications content. There are also ever-increasing levels of technology-enabled crime and cybercrime such as child exploitation and online fraud for which historical, internet based non-content telecommunications data is critical evidence.

The current legislative arrangements institute a justifiable compliance regime on Intercepting Agencies in order to ensure accountable use of powers. However, like other facets of the legislation this regime has not kept pace with changing technology and aspects of it have become unnecessarily complicated and onerous, requiring substantial police resources. This inquiry presents an opportunity to modernise the regime to ensure accountability and privacy measures remain relevant.

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

   a. the legislation's privacy protection objective

The AFP believes that the right to privacy and freedom of expression, the fundamental principles underpinning the TIA Act, must be retained. Both interception agencies and relevant industries have a role in protecting these rights for all consumers of telecommunications and internet services.

Whilst the safeguards prohibiting unlawful access to communications need to be retained government must also ensure that agencies' ability to continue to effectively and proportionally intercept and access communications does not face further decline. In line with this lawfully obtained information must also be protected and the agencies which have access to it must remain accountable for the way it is collected and used.

b. the proportionality tests for issuing of warrants

Proportionate and justified use of interception powers are cornerstone concepts on which the TIA Act is founded and the AFP works in adherence to these principles however, the current formulation to determine what is justified is becoming increasingly out of balance to the changes in the way people communicate, the technology available to communicate and the use of that technology to commit crime.

The justified proportionality in the use of powers under the TIA Act is currently determined by balancing the needs of the investigation against the interference to an individual's privacy. This is undertaken by assessing a range of factors such as the lack of availability of evidence from other investigatory methods and how useful the evidence likely to be gathered from the content of the communication or data might be. The AFP sees benefit in strengthening the existing proportionality test to include consideration of the overall community good served by the investigation for which the interception is sought.

Another main element of this proportionality and justified use approach that will benefit from review is the definition of serious offences for access to communications. The core of the definition in section 5D of the TIA Act limits interception to support the investigation of a serious criminal offence, generally with a penalty of at least seven years jail.

The complexity of section 5D does not adequately address certain crime types such as child exploitation and grooming offences, the emergence of cybercrime offences involving the use of computers or telecommunications networks to threaten national security and ancillary offences to serious and organised criminal activity. This is potentially out of step with community expectations that law enforcement should be able to effectively use interception to investigate these serious matters in a proportionate and justified way.

c. mandatory record-keeping standards

The TIA Act currently contains extensive requirements for agencies to keep records in relation to telecommunications interception, access to stored communications and disclosure of non-content telecommunications data. The objectives of these requirements are to ensure that agencies keep records that:

- Create an audit trail;
- Indicate how warrants were executed;
- Detail how information was used, and
- Can be used in evidence to protect sensitive methodology.

There are however directives within the TIA Act which in 2012 no longer serve a clear and necessary function. For example the TIA Act includes a requirement that all C/CSP's must receive a certified copy of each warrant. The original function of this process was to ensure carriers were basing interception on lawfully issued warrants. This is redundant given that high quality copies of documents can be sent via facsimile and e-technology. As well as being costly and time consuming this transfer of documents presents a potential risk to the security of warrant information as it must be transferred via mail and courier.

The AFP acknowledges that record keeping requirements and independent oversight are important ways for Parliament to ensure the public that the powers of the TIA Act are used lawfully.

The AFP has a strong organisational governance framework which all members must adhere to in the carriage of their duties; this extends to dealing with sensitive information.

In conjunction the AFP's robust governance framework specific to interception includes use of agency guidelines for Telecommunications Interception, Aide Memoire's, and specific authorisations restricting access to lawfully intercepted information to only those who require it for the performance of their duties.

Processes governing the administration of records associated with use of powers under the Act are subject to regular internal review; furthermore the AFP benchmarks its practises to guarantee that the AFP's own core values are being upheld.

The AFP believes the current legislated scheme needs review. It may have reached the point where it is too focussed on administrative requirements, rather than providing the basis for Parliament and the Ombudsman to ensure agencies are using the powers in the Act in a way that is consistent with the principles underlying the Act. There would be value in redrafting the legislation to include simplified, comprehensible and meaningful accountabilities and annual reporting obligations to enhance community understanding of the regime and its safeguards.

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

b. the standardisation of warrant tests and thresholds

Currently interception warrants have a base threshold of specified serious offences with a seven year imprisonment penalty threshold whilst stored communications warrants operate on a three year threshold.

The appropriateness of these separate warrant tests and offence thresholds should be reviewed taking into consideration the contemporary use of communications in society generally and by persons of interest in the commission of crime, and the nature of the technology underpinning telecommunications and internet communication services. A key example of this

is the increasing use of stored communication as a means of covert communication.

From a law enforcement perspective such a review needs to take into account the basis of the gravity of the conduct; the increasingly ubiquitous nature of telecommunications content and stored communications as evidence of the commission of an increasing number of offences that cause significant harm to the community, and the transitory nature of that content. It may be that the differentiation currently imposed between the two forms of content is no longer appropriate and that a reviewed and unified threshold would be more appropriate to meet both community expectations and law enforcements needs.

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

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

The TIA Act currently relies on complicated definitions of permitted purposes contained in section 67, 68 of the TIA Act for lawfully intercepted information, sections 139 for stored communications. These provisions regulate how the agency which intercepts, access stored communications or seeks non-content telecommunications data can share the information collected from these activities with other agencies. These rules are not uniform.

More flexibility exists for stored communications and non-content telecommunications data. The complicating factor for agencies from this approach is exemplified in the case of non-content telecommunications data. Agencies can do less in terms of sharing non-content telecommunications data collected as part of an interception warrant than they can do with non-content telecommunications data collected from an internal authorisation. The Committee should consider harmonising the approach to sharing and using information collected from interception, stored communications and internally authorised disclosure of non-content telecommunications data. The basis for this should be on the type of information being disclosed, not the way it is initially lawfully accessed.

The complex and evolving nature of transnational crime means that no one agency can effectively conduct complex investigations. Collaboration is an essential element in achieving operational goals. The TIA Act as it currently stands impedes the effective exchange of lawfully obtained communications information and reduces the efficiency of operational partnerships. Simplified, principle based use and disclosure rules would be more consistent with the modern approach to cooperation between agencies and assist in assuring information obtained under lawful interception is maximised appropriately to serve the public good.

The following case studies highlight current limitations to the AFP's ability to disclose information:

Case study 1 money laundering investigations

The AFP has conducted operations into money laundering where, during the course of extended investigations, evidence was obtained to indicate a person of interest was also involved in the commission of offences against the *Migration Act 1958.* Although DIAC is a regulatory body the lawfully obtained information could not be communicated to DIAC by the AFP for the establishment of a DIAC own investigation due to the TIA Act's rigid approach to applicable agencies. This meant the offences went unprosecuted.

Case Study 2 Sexual Servitude investigation

During an investigation into sexual servitude offences, lawfully intercepted information revealed the apparent commission of offences in relation to the fraudulent production of official documents.

Due to existing provisions within the TIA Act and limitations to the permitted purpose definition this information was not able to be communicated to the appropriate authorities for further investigation.

Case Study 3 Terrorist investigation

During a multi-jurisdictional and multi-agency investigation into Melbourne-based extremists plotting a domestic attack the sharing of information was imperative.

The extensive authorisations and processing required to comply with the rigid sharing provisions in the TIA Act were noted to impede the free exchange of lawfully intercepted information and knowledge otherwise customary in a dynamic and fast moving operational environment.

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

a. Creating a single warrant with multiple TI powers

Some of the complex provisions in the TIA Act particularly relating to emergency interception and telephone warrants cause significant operational difficulty, often in serious and life threatening situations.

Case study 4 Emergency Interceptions and procedural complexity.

In February 2009 ACT Policing officers were contacted by a male regarding the kidnapping of his underage sister by a person known to the family. Serious concerns were held for the welfare of the young woman.

Police set about initiating an emergency interception of the brother's service which the suspect had used been using to contact the family. Currently the use of emergency provisions is legislatively limited to occasions where consent has been obtained and whilst initially supportive the family became uncooperative when Police Negotiators requested the signing of a consent form. The brother then expressed a desire to find the offender himself and handle the situation according to his cultural tradition.

> In light of this Police opted to make an emergency telephone application for a warrant. These applications can only be made by officers delegated by the Commissioner in writing. Once an appropriate officer had been identified and the warrant obtained valuable evidence had already been lost.
>
> A further complexity was encountered when the applicant tried to present the affidavit and signed copy of their delegation to the issuing authority on a weekend which was within 48 hours after the warrant was issued (as stipulated in the TIA Act.) The issuing authority declined to receive the documents in the erroneous belief that the legislation acknowledged only business days. This failure to meet the time parameters delineated in the TIA Act rendered the warrant non-compliant and the evidence obtained open to challenge.

This example is not unique. In any one financial year a number of warrants will be issued in good faith and on a sound basis but inconsistencies render them invalid and necessitate revocation and replacement applications. This becomes costly for agencies and time consuming for issuing authorities.

Other out-dated legislated requirements such as sending certified hard-copies of issued warrants to carriers following interception represent a potential security risk that is unnecessary now that carriers are able to receive high quality copies of this same information via electronic means.

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

14. Reforming the Lawful Access Regime

a. expanding the basis of interception activities

When the TIA Act was written in 1979 it was simple to establish a straightforward link between a person and a form of communication, customarily based around a telephone number. Therefore warrants that currently authorise interception do so on the basis of:

- A service being used or likely to be used by a suspect;
- A service that is the means or is likely to be the means by which a person sends communications to or receives communications from a suspect; or
- A service or device used by a suspect.

That industry environment no longer exists. Several service or application providers may be involved in any one communication event. Individuals often use multiple devices and applications to communicate and free accounts can be established quickly and with no clear connection to a real life identity. Further, the current approach presupposes that the communications are between people using devices, not machine based communications as may be used through botnets or other internet based crimes where communications content is an important source of evidence. Into the future, given the move from circuit based

to IP based telecommunication services, identifying communications between persons will become increasing challenging.

In light of this it is no longer viable to continue to base interception solely on the traditional network identifiers prescribed in the TIA Act. For this reason the AFP considers additional basis for interception such as the concept of communications of interest that relate to the offence under investigation would be of benefit. . This concept could include the source of a communication, the destination of a communication, and the type of communication.

The following case study illustrates why the basis of interception needs review.

Case study 5 – Complexity identifying communications and high content-data volumes

In a recent Counter Terrorism investigation, a notification under a named person warrant was obtained to intercept both voice and content-data from an IP. High volumes of traffic being received in the pre-existing dedicated internet based interceptions meant the accommodation of the lawful intercept had to be delayed to allow for systems upgrades.

On commencement it became apparent that the notification was not addressed to best identify the content of interest and the IP could not configure the interception to capture the internet content required by the investigation.

The investigative time expended in monitoring extraneous content such as IP Television had an adverse impact on the resources available to dedicate to progressing the Operation. If the TIA Act made it possible to exclude specific streams of traffic and target only those communications identified as high value then resources could be more effectively deployed.

Case Study 6: Better Targeting of Communications

An AFP/NSWCC/NSWPol taskforce investigation into a crime syndicate involved in money laundering and the importation of cocaine concealed in volcanic rock paving tiles.

Physical surveillance observed a member of the syndicate in Melbourne using a laptop on multiple occasions at varying locations known as ‘hot spots’ providing free or low cost WiFi internet access.

Intelligence was able to establish email addresses and an encrypted Blackberry as the chief form of contact with the syndicate in Mexico in addition the target’s operational tradecraft was sophisticated and no use of conventional telecommunication services (mobile calls, payphones, landlines) was made.

The current legislation restricted agencies from effectively intercepting the internet data, due to the constant movement of the target.

If it was possible to narrow the focus of the intercepted traffic by using characteristics including that of location, timing of appearance on Wi-Fi networks and the email address, interception of the targets internet traffic would be possible.

Such interception may well be conceivable if agencies were able to apply to modify the details on which warrant was based.

15. Modernising the Industry assistance framework

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

The TIA Act does not address encryption, as encryption was not a factor relevant to consideration the Acts inception. Encryption now, however, is a growing complication reducing the effectiveness of the regime and limiting the AFP's ability to interpret intercepted communication.

There are two broad means by which the many types of encryption are employed: passive (default) or active (user opt-in). The critical issue is that although it is possible for the AFP to collect encrypted communications these communications are impenetrable as they cannot be reconstructed in viewable form.

The challenge of encryption is of particular community concern as unchecked it allows perpetrators of serious crimes to avoid detection by concealing their actions behind sophisticated technological apparatus.

In response, law enforcement needs another lawful way, other than by consent, to seek assistance to decrypt lawfully intercepted information, stored communications and non-content telecommunications data.

The criminal law has addressed encryption in relation to the seizure of electronic evidence. Section 3LA of the *Crimes Act 1914* sets out provisions regarding information obtained under search warrants. It allows a police officer to apply to a magistrate for a warrant to require a person to provide in accessible form data held on a computer or data storage device where the computer of data storage device has been seized under a warrant. The person to whom the warrant applies includes the subject of an investigation, the owner of the device, an employee of the owner, a relevant contractor, a person who has used the device or a systems administrator. Failure to comply with a notice attracts a penalty of up to 2 years imprisonment.

The use of encryption has been increasing across all serious crime types as more sophisticated encryption protocols are rolled out. Encryption is of specific concern in relation to Child Protection Operations where many criminals develop their own custom-made tools to avoid detection.

> Case Study 7: Hidden Networks and Peer to Peer exchange of encrypted content.
>
> During an investigation into an online paedophile network, it was noted that targets deployed a multiplicity of encryption techniques. They sent messages using an encryption overlay; images were encrypted and 'hidden' within other images which were then sent via closed peer to peer networks which also used encryption. Advanced Encryption Standards (AES) applications were used on virtual machines (computers within computers). The combined effect meant persons of interest were able to browse the internet without leaving detectable forensic footprints for investigators.

> Additional members of this network identified and pursued in a related operation took the anti-forensic techniques further and used full disk encryption along with hidden volumes that were disguised using a technique that allowed for plausible deniability of the content, effectively circumventing both interception and search warrant legislation.
>
> Persons of interest identified in the investigation included a computer anti-virus developer, and a computer networking trainer; their technical expertise was such that they were able to develop and customise their own encryption protocols rather than relying on off the shelf products.

A review of the TIA Act to include provisions for the issue of lawfully binding decryption notices would help the AFP as it would be possible to lawfully compel those who write their own encryption to provide access to clear communication. It would also offer those who provide commercial encryption protocols lawful protection when providing assistance. The AFP is able to provide additional cases studies in camera.

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

Disclosure of non-content to telecommunications data for law enforcement purposes is currently regulated by Chapter 4 of the TIA Act, which permits agencies to authorise the disclosure where it is reasonably necessary for the enforcement of criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. Chapter 4 also contains separate provisions enabling access for national security purposes.

Non-content telecommunications data is an important investigative tool for the AFP. It can provide important leads for agencies, including evidence of connections and relationships within larger associations over time, evidence of targets' movements and habits, a snapshot of events immediately before and after a crime, evidence to exclude people from suspicion, and evidence needed to obtain warrants for the more intrusive investigative techniques such as interception or access to content.

Disclosure of non-content telecommunications data is one of the most efficient and cost effective investigative tools available to law enforcement. There are no operational risks, and from a law enforcement perspective and as it relates to data about communications rather than its content, it raises fewer privacy concerns than the other covert investigative methods.

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

Industry has acknowledged that, in evidentiary terms, non-content telecommunications data can be as important as, or more important than, telecommunications content. However, despite the increased reliance on data

and the acknowledgement of the importance of data, industry has confirmed that there will be degradations in the type of non-content telecommunications data which will be retained into the future. They indicate that this is a natural evolution as a result of advances in technology and business models. For example, the telecommunications sector is quickly migrating from the traditional telephone network to IP based networks. Traditionally, telephony services retained detailed billing information on who called who, when and where, and the time of each call. Internet based service providers tend to charge on the quantity of data used rather than on a per call basis. Over time, as telecommunications services such as voice-telephone migrate to voice-over-internet based services, less and less information will be retained and stored. This includes data that currently provides law enforcement agencies with a key method of tracing communications that can reveal associations between members of criminal organisations. Therefore, this means that traditionally available non-content telecommunications data—as: 'Person X called person Y at this time'—may no longer be available.

The development of a data retention proposal is intended to ensure a national and systematic approach is taken for the availability of non-content telecommunications data for investigative purposes. Data retention would not give agencies new powers. Rather it would ensure that existing investigative capabilities remained available and were adapted to these changes in industry. The TIA Act provides a high level of accountability and strict access requirements to obtain telecommunications information. These constraints recognise the responsibility of government to manage the competing interests of privacy and the expectations of the community that unlawful activity will be investigated and prosecuted, as well as the important role that the telecommunications industry plays in supporting law enforcement and investigative activities.

A data retention scheme would also address current gaps and improve consistency in the retention of data by C/CSP's as the data they currently retain and provide to law enforcement is determined by their individual systems architecture and business models.

The volume of data and its retention by Internet Service Providers (ISPs) for use as evidence presents challenges. This mainly relates to metadata —the records of a call or IP information.

Non-content communications data is of key importance in assisting investigations but in the modern landscape there is differentiation between the types of non-content data sought and used for investigative purposes.

Access to subscriber or account holder data is comparable in intrusiveness to open source information such as traditional fixed line telephone directories. It aids law enforcement in obtaining information to help establish further avenues of inquiry. For IP's where there are no analogous provisions to the directory service concept this non-content communications account data is imperative.

Access to historical non-content traffic data can be vital as it is one of the few tools available to law enforcement that can assist in retrospectively establishing a timeline of an event or series of communications. In some circumstances it has

been used to show links between persons of interest and victims of crime and can rule out individuals from further investigation, avoiding the need for the use of more intrusive surveillance and costly deployment of resources.

Prospective or real time access to non-content communications data is of immediate operational value as it offers the ability to collect traffic data relating to a person of interest suspected of a specified offence as it is created.

> *Case Study 8: Use of prospective data to assist investigations*
>
> During 2010 an Operation obtained prospective call associated data (CAD) Authorisations in relation to a person suspected of war crime offences *contrary to section 7(2)(a) of the Geneva Conventions Act 1957, namely torture, inhuman treatment and wilfully causing suffering or serious injury.*
>
> The suspect was wanted for extradition to Croatia to face trial for these offences and was attempting to avoid location.
>
> The AFP's CAD Authorisations did not involve the provision of any content of the suspects communications however the information the non-content data provided investigators regarding the general geographical location of the targets mobile handset was instrumental in assisting the AFP successfully locate the target.

The AFP appreciates that this form of access to non-content communications data whilst less intrusive than a content based interception should still be subject to appropriate accountability.

In summary, the implications for Law Enforcement if non-content telecommunications data is not retained:

- Limited ability to track and pursue offenders in a timely and effective way;
- Limited ability to conduct thorough and complete investigations;
- Inability to present best evidence to courts;
- Inability for police to react to some life threatening situations;
- Inability to follow through on potential leads and gather evidence and identify criminals, and
- Ability for criminal enterprises / organised crime groups to exploit this vulnerability.

Conclusion

Technological advancements in the communications sector have led to considerable improvements in the lives of ordinary Australians and have seen profound change to the way we live and connect. The AFP embraces the benefit of these changes. Whilst technology has made life easier it has also created new

crime types and enabled new ways of conducting existing criminal activities. In the face of the challenges presented by this changing environment the AFP recognises that it is essential to adapt in order to meet Government and community expectations to combat serious and organised crime. To do this we need legislative reform that provides ongoing support of our existing capabilities ensuring we have effective powers now and into the future.

In the absence of urgent reform, agencies will lose the ability to effectively access telecommunications content and data, thereby significantly diminishing the collective ability to detect, investigate and prosecute threats to security and criminal activity. The diversification of the sector and technological change mean that while a greater array of non-content communications data is being created increasingly less is being retained. This negatively impacts investigations and is exploited by individuals involved in the commission of a range of serious offences including cybercrime, terrorist activity and the exchange of child exploitation material.