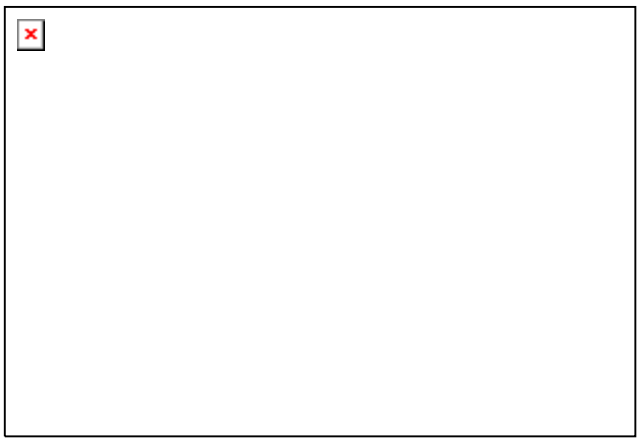
# Submission No 200

## Inquiry into potential reforms of National Security Legislation

**Name:** Gavan Segrave
Detective Inspector

**Organisation:** Victoria Police
St Kilda Rd
Melbourne 3004



# Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into Potential Reforms of National Security Legislation.

**7th September 2012**

# Index

## Submission to the Parliamentary Joint Committee on Intelligence and Security on Potential Reforms to National Security Legislation.

---

### *Introduction*

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is to inquire into potential reforms of National Security Legislation and has called for written submissions including those from law enforcement agencies around the nation. Victoria Police is pleased to provide such a submission. While several different pieces of legislation will be reviewed by PJCIS, modernising lawful access to communications and associated communications data pursuant to the Telecommunications (Interception and Access) Act 1979 (TIA Act) has the most application to Victoria Police and will form the basis of this submission.

The TIA Act was drafted and came into being in 1979. Victoria Police has had the legislative ability to intercept telecommunications services since 1988, as a consequence of the introduction of the enabling Telecommunications (Interception) (State Provisions) Act 1988. In this era, interception was conducted solely on landlines to capture conversations made by suspects involved in serious crime. Analogue mobile phone use was still in its infancy and there was no technological capability to intercept communications made by mobile phones until the early to mid 1990's. The ability to communicate by SMS was also introduced. In the mid to late 1990's digital technology replaced analogue and again law enforcement was restricted for some time due to the inability to intercept this type technology.

As time progressed and further advances in technology were made, mobile phones became affordable, convenient and are now commonplace. The use of such technology is no longer restricted to voice and SMS. As noted in the Australian Communications and Media Authority Communications Report 2010-11 (the ACMA Report), consumers are diversifying their use of communications which has led to the increased use of voice over internet protocol (VoIP), the internet and alternative communication methods such as social networking in addition to using fixed-line telephones.

The ACMA Report further reveals that:

- the number of fixed-line voice services and call volumes continues to decline;

- the use of VoIP grew, with significant numbers of consumers using VoIP over mobile phone handsets;
- a net growth in mobile phone services in addition to existing mobile phone users upgrading to smart phones on the back of a sustained increase in adoption of mobile internet services;
- mobile numbers increasingly used for devices with wireless internet connectivity and for machine-to-machine communication.

The telecommunications landscape has changed extensively since the inception of the TIA Act, which in turn has undergone numerous amendments over the years in an attempt to try and stay abreast of and reflect such change. The law enforcement context in which the TIA Act is applied has also seen significant change over the last decade, in large part as a consequence of a series of large-scale terrorist attacks and attendant threats against western democracies. A key element of this new law enforcement context is what the Australian Crime Commission (Organised Crime In Australia 2011) has described as '*the confluence of organised crime, terrorism and corruption* (creating) *an enabling environment for moving and exchanging drugs, arms, people, stolen or pirated goods and for funding criminal and extremist activities*'. The ACC has reported that '*often the same routes, networks and methodologies are used for these activities*' and this convergence is of most concern '*when it is married with the increasingly blurred distinction between the politically-motivated activity of some terrorist groups and the criminal activities that fund them*'.

Even in the context of such fundamental change to the law enforcement environment, Victoria Police remains committed to the TIA Act's key objective of protecting the privacy of users of telecommunications services. However, Victoria Police believes that urgent reform of the TIA Act is now critical if law enforcement is to maintain an adequate investigative capability in terms of telecommunications interception and associated avenues of enquiry. The following commentary and case studies are designed to highlight to the PJCIS the types of operational challenges Victoria Police routinely face as a consequence of gaps and / or shortcomings in the current TIA Act, as well as demonstrate the benefits of telecommunications interception and data access in assisting to solve serious crime in this state.

## *Importance of telecommunications interception and access to historic and prospective data to Victoria Police criminal investigations.*

The Victoria Police mission is to provide a safe, secure and orderly society by serving the community and the law.

Telecommunications interception is a highly valuable and effective investigative technique employed by Victoria Police to combat serious crime in this state. Its use is critical and cannot be replaced by other investigative methods. Victoria Police recognises the impacts on the privacy of the individual, and has implemented strict internal policies and controls to coincide with stringent TIA Act requirements and oversight by the Special Investigations Monitor and Commonwealth Ombudsman ensuring access to information is restricted only to those who specifically require it in the context of the legislation. However, the TIA Act imposes no obligation on those who are served with material post investigation such as courts, defendants/defence counsel and the Office of Public Prosecutions. Before an issuing authority can grant a warrant, there are a number of matters that must first be considered including other investigative techniques used or available to investigators. Victoria Police is proactive in ensuring all available methods of investigation are considered and used where possible, prior to any warrant application.

The lawful use of non-content data such as subscriber information and call records accessed pursuant to section 178 of the TIA Act is crucial in terms of the intelligence and evidence gathering required before access to prospective information and/or a telecommunications interception warrant is applied for. It is a legislative requirement to demonstrate to an issuing authority that the suspect is utilising the particular telecommunications service and the likelihood of evidence being obtained in relation to the targeted serious offence. Subscriber information and call records data is invaluable in this regard. All requests for access to such data are first approved by an officer authorised pursuant to Section 5AB(1) of the TIA Act who is responsible for satisfying themselves the request meets the necessary thresholds. Victoria Police has stringent standards in terms of dealing with such information.

As carriers change their business practices from billing based on volume/length of calls made to billing based on data volumes, the need for carriers to retain such data is diminishing. This has enormous implications for law enforcement agencies reliant on this data to target suspects involved in serious crime.

Victoria Police commonly uses telecommunications interception during investigations into large scale drug trafficking, murder, kidnapping and serious armed robberies with often outstanding results. It was used extensively by the Purana Taskforce to combat a spate of murders and organised crime activity, which resulted in convictions for a number of criminals and prevented further murders taking place. It was instrumental in the capture of a notorious criminal identity who had fled the country while facing sentencing on serious drug charges.

Telecommunications interception has also proven invaluable in helping investigate cases which otherwise may not have been solved.

*Case Studies - Importance of telecommunications interception in criminal investigations*

Refer to Case Studies 1-3 in restricted attachment.

*Case Study - Importance of stored communications in criminal investigations*

Refer to Case Study 4 in restricted attachment.

## *Standardising warrant tests and thresholds.*

### Definition of Serious Offence

The definition of *serious offence* pursuant to section 5D of the TIA Act is long, complex and outdated and it excludes offences which should be so classified. There are offences Victoria Police routinely investigates that are serious in nature, but are not specified in the definition or only become serious offences if they meet certain additional conditions such as being part of a series of offences, involve substantial planning and organisation and sophisticated methods and techniques.

Offences that are serious in nature but are not captured in this section include blackmail and perverting the course of justice, where an investigative method such as telecommunications interception would assist in the investigation of offenders charged with serious crimes attempting to arrange false alibis or have witnesses change their statement and/or provide false evidence.

Offences including theft, handling stolen goods, extortion and dealing in firearms only become *serious offences* when the additional criteria is met including the requirement for the circumstances to involve the use of sophisticated methods and techniques. This particular component often precludes investigators from using telecommunications interception as a viable investigative technique.

Extortion is a crime that occasionally satisfies the two or more offender criteria but seldom involves substantial planning and organisation and almost never meets the sophisticated methods and techniques test. Telecommunications interception should be a logical avenue of enquiry against suspects involved in these types of crimes but this has not been an option.

Section 5D(7) requires that persons acting as accessories to crime may only have their telecommunications intercepted when the original crime is specified in 5D(1) - murder, kidnapping or terrorism. Accessories to other serious crime are not able to have their telecommunications intercepted.

These issues impact on the obligation of Victoria Police to provide a safe, secure and orderly society in the following ways:

- evidence unable to be gathered
- delay in solving crimes
- crimes being unsolved.

A simple solution would be for a *serious offence* to be defined on the basis of the penalty it carries - offences punishable by imprisonment of a certain number of years should be classified as *serious offences*.

*Case Study - Serious Offence definition (dealing in firearms)*

Victoria Police investigators were investigating a prominent Melbourne based organised crime figure for dealing in firearms. Intelligence suggested the suspect was flying to Sydney on a regular basis for the purpose of purchasing firearms for redistribution into Melbourne.

Surveillance revealed the suspect met on several occasions with Sydney based organised crime figures who were themselves suspected of dealing in illegal firearms.

Investigators were able to obtain call charge records on the suspect's telecommunications service pursuant to Section 178 of the TIA Act. This showed contact between all parties leading up to, during and after the suspect's visits to Sydney.

The method in which these firearms were being conveyed to Melbourne was unknown. In order to obtain evidence against the suspect, investigators believed a telecommunications interception warrant may assist.

Section 5D of the TIA Act determines the offence of dealing in firearms or armaments is a *serious offence* but only where it involves, amongst other things, the use of sophisticated methods and techniques. As this particular criterion could not be met, a telecommunications interception warrant was unable to be applied for.

Other investigative techniques were considered but deemed unsuitable. As a result, it was not possible to progress this particular investigation and it lapsed.

*Case Study - Serious offence definition (theft)*

In two unrelated instances in recent times, Victoria Police investigators were attempting to solve the theft of approximately $250,000 cash from Automatic Teller Machines (ATMs). Suspects for these crimes were employed by security companies servicing the ATMs.

It was established that access to the respective ATM was made using a key. Investigators also established there was an accomplice involved in both offences.

A number of investigative methods were contemplated in an attempt to solve the crime. Investigators identified telecommunications interception as the most appropriate technique to gain evidence implicating the suspects.

Section 5D of the TIA Act determines the offence of theft is a *serious offence* but only where it meets additional criteria such as the offence being committed in conjunction with other offences of a like kind and involves the use of sophisticated methods and techniques. The offences were unrelated and a "once off" so there were no other offences of a like kind. The use of a key cannot amount to sophisticated methods and techniques being used. As a result, telecommunications interception was not possible. These crimes remain unsolved.

*Case Study - Serious Offence definition (accessory to a serious offence)*

Victoria Police investigators commenced an investigation into significant injuries sustained by an infant child. The suspect for this offence was the boyfriend of the child's mother. While the mother was not suspected of being involved as a principle offender, investigators established she was trying to assist her boyfriend by providing an alibi believed to be false.

The suspect's telecommunications were able to be intercepted but not the child's mother as it did not fall within the definition of section 5D(7).

## Access to telecommunications data

Lawful access to existing information or documents for the purpose of enforcing the criminal law or locating a missing person can be made pursuant to sections 178 and 178A of the TIA Act respectively. Access to prospective information or documents for the purpose of investigating an offence that is punishable by imprisonment for at least 3 years can be made pursuant to section 180 of the TIA Act. Victoria Police investigators have found that certain situations arise that do not allow for access to data where it would be of great benefit.

### *Access to data (parole violators)*

Victoria Police has a dedicated team responsible for the co-ordination of reporting parole breaches to Corrections Victoria and the execution of warrants to arrest those whose parole has been revoked by the Adult Parole Board. Some parolees commit serious offences while going to great lengths to avoid arrest and being returned to prison. In these circumstances, investigators have been able to utilise existing legislation under S.178 and S.180 to locate, arrest and charge the offenders for these post parole offences and return them to custody. Investigators describe the ability to do this as invaluable.

However there are many cases where persons have breached their parole for reasons other than criminal activity and are avoiding arrest. Examples of this include breaching reporting requirements, residential conditions, curfews and consorting bans. In this regard, investigators have been unable to utilise the provisions of sections 178 or 180 to aid in the parolees' capture and return to prison. Access to data would assist in locating these people in a timely manner, thus reducing harm to the community by way of reduction in crime and so meeting community expectations.

### *Access to data (missing persons)*

Law Enforcement Agencies have the legislated ability to access existing information such as the telephone records of missing persons. While this is of value, there is a need for access to prospective data to provide a greater ability to locate persons reported as missing. Currently, the only avenue available to agencies such as Victoria Police to obtain prospective data for a missing person is pursuant to S.287 of the Telecommunications Act 1997 in circumstances where the disclosure or use of the information is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person. The overwhelming majority of cases do not fit these criteria as it cannot be shown that any threat to these persons is imminent.

As such, Victoria Police has been unable to utilise what would be an effective means to locate missing persons - including those who are lost, disoriented, mentally impaired, elderly or injured.

## *Simplifying the information sharing provisions that allow agencies to cooperate*

The TIA act has stringent measure to protect lawfully intercepted information obtained under a telecommunications warrant. It regulates how such information can be used and if necessary shared between agencies. Criminals involved in serious crime often do so on a national basis, thus necessitating a multi-agency investigative response. Collaboration between agencies is essential. It is not uncommon for Victoria Police, especially in joint taskforce situations, to provide/receive information to/from other law enforcement agencies for the purposes of investigating serious offences. Victoria Police considers the particular legislation governing sharing of information between agencies to be somewhat complicated and in need of simplification.

While it is important that there are strict controls over the sharing of information, Victoria Police investigators have on occasion found the legislation to be too restrictive. There have been instances where lawfully intercepted information would be of high importance to other organisations providing a function in the service of the community, but Victoria Police is legislatively prevented from providing it. For example, if an interception identifies that a child is at risk of harm from its parents, this information cannot be communicated to child protection agencies. Similarly, where investigators identify the inappropriate dealings of a prison officer, this information cannot be passed on to prison authorities.

## *Streamlining and reducing complexity in the lawful access to communications regime*

The TIA Act stipulates that applications for telecommunications interception warrants are to be made in writing and be accompanied by an affidavit setting out the facts and grounds on which the application is based.

In urgent circumstances where it is impracticable to apply for a warrant in this manner, the TIA Act allows for an application to an issuing authority to be made by telephone and the relevant documentation provide by the following business day. It is not an infrequent occurrence for Victoria Police to make such applications, particularly in the context of time-critical and dynamic investigations such as kidnappings. The requirement to make the application solely by telephone has proven to be impracticable and inflexible. The ability to make such an application in person should be considered. There have been instances where an applicant has been in the close proximity of an issuing authority. Instead of making an application in person, they have sat in their motor vehicle or in an adjoining room and made the application by telephone before making their way to the issuing authority to have the warrant signed.

Additionally, with the impending introduction of the Office of Public Interest Monitor to Victoria, an increased level of flexibility in terms of the process for the making of urgent telecommunications interception applications would be of great benefit to all parties to such applications.

## *Creating a single warrant with multiple TI powers.*

When the TIA Act was first drafted, it was typical for a suspect to be utilising a single service (landline). Telecommunications now take place in many ways including email, social networking and other internet transactions, most of which are available through ‘smart’ phones. Accounts can be set up quickly and anonymously. Suspects are utilising these avenues to communicate with others about their criminal activities.

Victoria Police staff who monitor the communications of suspects under warrant frequently hear calls where suspects, during the course of a conversation, will inform or infer to the other person that they will discuss “other matters” or arrange meetings over other forms of communication. Frequent references are made to using other ever increasing new technologies precluded from interception.

It is common practice for criminals to use numerous Subscriber Identity Module (SIM) cards and rotate them through a single handset in quick succession in an attempt to thwart interception. Victoria Police conduct investigations, most typically high level drug investigations, where this approach is routinely used by targets.

It is no longer practicable for warrants to be obtained solely on traditional network identifiers such as telephone numbers or IMEI numbers. A single warrant in which particular identifier(s) could be stipulated (such as a username, webmail address, internet account) would enable the targeting of communications of a suspect without the need for multiple warrants over time on the same target.

*Case Study - Criminal investigation hampered by warrant regime*

A prisoner was orchestrating serious criminal activity outside gaol by communicating with non-incarcerated persons. The methodology used by the prisoner was to manipulate the existing prison phone system and protocols by using an external party to forward the prisoner's calls to criminal associates.

A warrant pursuant to Sections 46 and 46A was not applied for due to the likely significant impact to the privacy of other parties not involved in the investigation such as other prisoners and prison staff using the service. A warrant pursuant to Section 48 was also unable to assist due to both legislative and technical constraints.

Intelligence suggested the prisoner solely used this process to discuss criminal activity and there was a strong likelihood that significant evidence of the prisoner's involvement in serious offences would have been obtained had an interception warrant been able to be obtained. As a result, investigators were unable to obtain sufficient evidence to meet the evidentiary threshold to proceed with criminal charges against the prisoner.

A warrant based on a broader communication identifier that covers the current spectrum of Sections 46, 46A and 48 in relation to the target of the investigation would have allowed the investigation to proceed without impacting on the privacy of persons not involved in the investigation.

## *Extending the regulatory regime to ancillary service providers not currently covered by the legislation.*

The range of providers of telecommunications services to Australian consumers has risen dramatically in recent years and continues to grow. Some of these providers are based in this country enabling compliance with the current regulatory regime. However, the majority of popular services are from offshore providers.

Monitoring of intercepted communications by Victoria Police routinely demonstrates that services such as these are being used by suspects in furtherance of their criminal activities. Without a mandatory regulatory obligation placed on the providers of these services used in Australia, criminals can continue to communicate without the risk of being exposed to interception. There needs to be legislative parity with the obligations applicable to Australian service providers.

It is imperative that all providers of communications services to Australian consumers not only have the capability of servicing lawful requests by law enforcement agencies but the ability to provide content as specifically requested. For example, if an agency is interested only in intercepting certain parts of internet activity, say emails, it should be possible to receive only this content and not the whole gamut of activity. This approach targets the communications of interest and not a blanket approach thus significantly reducing privacy implications and the resource intensive process of monitoring and deciphering superfluous content.

*Case Study - Criminal investigation hampered by inability to obtain content from ancillary service provider*

An investigation into sexual offences against a child involved a suspect utilising non-traditional methods of communication (Facebook). As investigators obtained information that showed such communication had taken place, they sought to obtain evidentiary material through Facebook. The existing process for obtaining this information through the Mutual Legal Assistance Treaty with the United States and the significant delay it caused, forced investigators to abandon that particular avenue of enquiry.

As a result, no direct evidence was obtained from the primary communication method utilised by the suspect. This resulted in a large “gap” in evidence against the suspect. The ability to intercept communications made through offshore service providers would have greatly assisted in this instance.

## *Establishing an offence for failure to assist in the decryption of communications.*

The types and volume of non-traditional telecommunications has increased exponentially over recent years as has the volume of providers providing these vast ranges of services. The use of these services, most of which are accessed through offshore providers, is now commonplace including by those committing serious criminal offences.

Data obtained under telecommunications interception warrants for a wide range of offences increasingly contain material that is indecipherable by investigators due to encryption - thus reducing the effectiveness of the warrant. Encryption is not addressed in the TIA Act.

Monitoring of intercepted telecommunications has uncovered many instances where such services are used by suspects to discuss and exchange information in relation to their activities, safe in the knowledge the content cannot be decrypted by law enforcement. If this trend continues without being addressed, it is likely the value of telecommunications interception will significantly diminish in the future.

Some form of mandatory obligation, such as a legally binding 'decryption notice', is needed to compel providers of these services in Australia to allow for the interception and deciphering of such content. This would mitigate the increasing amount of indecipherable data being encountered, and foil those seeking to use encryption to hide their criminal activities.

*Case Study - Corruption investigation hampered by encryption*

A suspect in a corruption investigation by Victoria Police was the subject of a telecommunications interception warrant. During the course of the warrant, a number of intercepted communications proved indecipherable. These transactions involved internet based product (IP) and were encoded/encrypted.

Investigators strongly suspect the indecipherable communications, made over a mobile phone, contained evidence of the suspect's involvement in the targeted offence, as inferred by other intercepted conversations/SMS.

Investigators were unable to gain sufficient evidence to prosecute the suspect for the targeted offence.

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

Due to evolving business practices, telecommunications service providers have forecast the decline in the need to keep certain types of non-content data in the future. Providers of traditional telephone networks required detailed data for billing of its customers. Due to the migration to IP based networks, providers are billing customers on volume of data rather than on a per call basis.

Non-content data such as subscriber information and call records play a vital role in the investigative process. It enables investigators to link suspects to services, identify associations and identify a suspect's movements at a particular point in time such as when a serious offence was committed. It also has the ability to exonerate those initially considered under suspicion. It also aids other forms of covert investigative methods, such as surveillance. The use of non-content data as persuasive evidence in criminal trials is a common occurrence. Information gained through access to this data is always used in the normal application process for a telecommunications interception warrant.

Applications for access to non-content data are made in accordance with the requirements stipulated in sections 178 and 180 of the TIA Act.

Unavailability of data for investigations

Victoria Police investigators are constantly frustrated by the inconsistency in data retention periods between different carriers/carriage service providers. Investigations should not be hampered by the unavailability of data from one provider that would have been available had another provider been used.

Often, the incoming data from calls/SMS are crucial to the investigation of crimes such as stalking and breaching family violence intervention orders. These investigations are being hampered, or in many cases are unable to progress at all, due to the purging of such information from carrier's systems at the earliest opportunity.

Carriers do not keep cell tower information for long and again, it varies from carrier to carrier. It is not uncommon for investigators to have the need to establish whether a particular suspect was in a certain area at a certain period of time. This type of information is often necessary for reasons such as establishing whether they have identified a legitimate suspect and disproving alibis.

A consistent and extended data retention scheme by carriers/carriage service providers would greatly assist investigators in solving serious crime in this state. The security of telecommunications industry customer data should already be of the utmost importance. However, in light of recent breaches of telecommunications industry security, some form of legislative compliance framework to obligate them to protect their networks to the necessary standard may be considered. Law enforcement should have no role to play in this due to a clear conflict of interest.

The length of time stored communications data is available widely differs from carrier to carrier. The opportunity to obtain crucial evidence is often lost in a short period of time.

For example, allegations of sexual assault are often not immediately reported to police. It can sometimes be years after the commission of the offence before an allegation is made, especially where the victim was a child at the time of the offending. The inability to obtain telecommunications data in such circumstances can prove pivotal to the investigation.

A mandatory and consistent data retention scheme does not provide law enforcement with additional powers. It merely ensures that an important existing investigative tool remains available. The community expects that serious crime is investigated and wrong-doers are prosecuted. The telecommunications industry has an important role to play in supporting law enforcement in this regard.

*Case Study - Data Retention (Stored Communications) - corruption investigation*

A corruption investigation revealed evidence of communications by way of SMS messages between a police member and a member of an Outlaw Motorcycle Club. The content of the messages was reasonably believed to have contained evidence directly implicating the police member with criminal activity and coincided with particular key dates that the police member was suspected to have been involved in criminal activity. However, the existence of the messages was only established several weeks after the suspected criminal activity.

Despite investigators acting swiftly, the data relating to the communications had been deleted by the carrier. There was insufficient evidence to mount a criminal prosecution against the police member.

*Case Study - Data Retention (Stored Communications) - murder investigation*

Victoria Police investigators were investigating the stabbing murder of a male. Call records showed recent contact between the deceased and telecommunications services utilised by two males. Further records obtained showed that on the night of the murder there were several text messages between these two males. Investigators seized a SIM card belonging to one of the males which contained a text message that appeared to implicate both in the murder. All other text messages between the two had been deleted. A stored communications warrant was unable to be applied for due to the unavailability of the content from the carrier.

One of the males assisted investigators and became a witness against the other male who was charged with murder. The accused claimed it was the witness' idea to carry out the murder but the witness disputed this. Having access to all of the text messages between the two may have confirmed either person's story.

The accused was subsequently acquitted at trial.

## *Conclusion*

The TIA Act was enacted in 1979 and has been the subject of numerous amendments over the years. As a result it has become convoluted and is not an easy piece of legislation to digest or use. It also presents a range of inadvertent challenges to law enforcement agencies, as outlined in the Attorney General's Department discussion paper and this document.

The ability of law enforcement agencies to intercept telecommunications content and data is vital to meeting community expectations in relation to the investigation and prosecution of serious crime. Arrest, prosecution and conviction figures documented in the TIA Act Annual Report 2010-11 confirm the value of using telecommunications interception and its importance to investigators of serious crime.

The suggested reforms would greatly assist law enforcement agencies to cope with changing technologies and the associated methodologies employed by those committing serious crime, while striking a balance with the need to protect the privacy of legitimate users of telecommunications services in Australia.