Submission No 148

Inquiry into potential reforms of National Security Legislation

Organisation: New South Wales Government

NSW GOVERNMENT SUBMISSION

Inquiry into potential reforms of National Security Legislation

Introduction

The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) was developed in 1979, a time when almost all telecommunications of interest to criminal investigations were simple analogue telephone calls made from one fixed-location telephone via landlines to another telephone, and the sole domestic carrier (Telecom) and the sole overseas carrier (OTC) derived revenue based on billing for line rentals plus individual non-local phone calls and kept records of all calls made. Since that time there have been significant changes such as the introduction of mobile telephone and internet services available to the general public. These challenges have attempted to be accommodated by small scale changes to the TIA Act, which have led to an increasingly long and complex TIA Act which no longer achieves its policy objectives.

The NSW Government supports many of the discussion paper's proposals to reform the TIA Act, but is of the view that the effectiveness of the TIA Act is being challenged at every stage of an investigation, and fundamental reform is therefore required, not to increase powers, but to ensure that existing powers are not rendered completely ineffective.

Given the breadth of the Terms of Reference, the general nature of the discussion paper, and the request for an entire overhaul of the TIA Act, the NSW Government believes that further consultation on all aspects of the discussion paper and the provided submission is vital. Consequently, this submission is made as an introductory submission to the issues, and considers it integral that further opportunity is given to provide more detailed recommendations. It is suggested that this initially be done by taking evidence from officers of NSW interception agencies where they will be able to provide detailed and operational information.

The NSW Government has commented on the proposals outlined in Chapter 2, 3 and 4 of the Attorney-General's Department's discussion paper. However, the NSW Government has focussed its attention on the proposals in Chapter 2, as telecommunications interception is a vital tool for effective law enforcement in NSW. In 2011-12, the four NSW agencies with powers to apply for telecommunications interception warrants (the NSW Police Force, New South Wales Crime Commission, Police Integrity Commission and the Independent Commission Against Corruption) were issued a total of 1761 telecommunications interception warrants, and lawfully intercepted information was used as evidence in 1180 convictions. However, it should be noted that the evidence obtained from telecommunications interception, in practicality resulted in more convictions as a plea of guilty obviates the need to tender the available lawfully intercepted information as evidence. An effective TIA Act is therefore a key tool for combating crime in NSW.

As the jurisdiction which employs telecommunications interception the most, the NSW Government believes that it can provide a unique perspective and operational experience to the Committee.

Chapter 2 – Amendments to the *Telecommunications (Interception and Access Act 1979)*

The NSW Government has structured its comments on the proposals in Chapter 2 around the life cycle of operations, the challenges faced by agencies at each of those stages, and what a revised TIA Act would need to reflect.

The overall objective arising from these suggestions is to apply the overall principles of the TIA Act when first drafted to the technological, operational, and cultural contexts that exist now. The suggested changes are based on, but not limited to, the specific examples raised below.

The purpose behind the *Telecommunications (Interception and Access) Act 1979*

The purpose of the TIA Act is to protect the privacy of communications, except when access is justified for particular law enforcement and security outcomes. The TIA Act prohibits the interception of, and other access to, telecommunications except where authorised in special circumstances. As the TIA Act does not contain an objects clause, it would be beneficial for a modernised purpose of the TIA Act to be developed.

Achieving that Purpose Now

While the discussion paper notes that there have been a number of changes which have affected the ongoing ability of agencies to adequately access communications, the NSW Government contends that due to fundamental changes to the way technology works, infrastructure and business changes, and importantly how enforcement agencies work, there is an unprecedented challenge to the ongoing effectiveness of the TIA Act in establishing an effective policy framework for the protection of privacy, and the appropriate use of communications to investigate serious crime.

Technological changes

Significant technological changes from when the TIA Act was drafted in 1979 include a shift from a telephone based communications system to an internet based system, the introduction of a vast number of telecommunication service providers, the rapid decline of call-based revenue generation and improved encryption.

Communication via the internet, such as voice over internet protocol (VoIP), emails, chat rooms etc are now all digitally encoded when sent and decoded upon arrival, providing a level of innate privacy. Although interception of the communications in their coded form is possible, law enforcement agencies are no longer able to decode for effective communications.

Communications are now rarely an uninterrupted signal, but instead exist as individual component 'packets' of data, travelling over internet-protocol networks. These packets move from one point to another via many different points, and move across the network by being copied and then forwarded on to the next point in the network.

In addition, communications are copied and recorded for a number of useful purposes, some by individuals, in the operation of their computers and other devices (e.g. virus scanners and email filters), some third party providers of similar services, and commercial approaches where information is tracked in order to be remembered when we visit particular websites, or to target advertising.

A further change of significance to law enforcement agencies is the increasing use of sophisticated technology by criminals. Organised criminals are now able to operate outside the reach of ordinary telecommunications interception, especially though internet-based communications systems and using sophisticated encryption. In addition, they utilise their own telecommunications interception capabilities.

Further changes to the technological environment must be anticipated with the development of the National Broadband Network. This is just one known imminent technological advancement, however more powerful means of electronic communication are constantly being developed, encryption will improve and volumes of traffic will increase. Not only must the TIA Act catch up, but it must "future proof" against rapidly emerging technologies.

Cultural changes

The rapid advance of technology since 1979 has resulted in a cultural shift, in particular through the use of the internet. Now, people can use the internet for almost every aspect of everyday life.

According to the Australian Bureau of Statistics (ABS), the percentage of Australian households with access to the internet at home has continued to increase, from 64% in 2006-07 to 79% in 2010-11[1]. The proliferation of 'smartphones' means that people can now use the internet on the move. At the end of June 2011, there were 9.7 million mobile handset subscribers in Australia able to access the Internet via mobile phone[2]. The internet is increasingly being used by individuals for banking, shopping, travel bookings, research, gaming, leisure, private hobbies, and written communication (emails, VoIP, chat rooms). The expansion of social networking also means that individuals share great quantities of personal information on social networking sites, including photos, interests, and events, and their location. In some cases information may be shared with the public, and in other cases it may be shared with a finite group of contacts. According to the ABS, social networking and online gaming was performed by 88% of internet users in the 15-17 years age group and 86% of internet users in the 18-24 years age group[3]. The transmission of videos, graphics, and other modern material means that the amount of data now transmitted is vast and able to overwhelm law enforcement resources. Investigatory material that may have once been obtained by a standard search warrant can now only be obtained through a telecommunications interception warrant. Without telecommunications interception law reform, the capacity of law enforcement agencies to engage in effective telecommunications interception will continue its current rapid decline.

Telecommunications interception law reform is needed not in order to increase the powers of law enforcement agencies but in order to reduce the decline in capability. If reform is not undertaken then criminal investigations in this respect will be put back to the era before effective telecommunications interception was available and potentially further, given the way that people now store information.

With the vast arrays of personal information now available through telecommunications, strong protection for privacy is necessary. It is recognised that an effective interception regime will need to be counterbalanced with effective privacy measures.

In considering how to protect communications, cultural shifts in relation to privacy need to be considered. The use of the internet enables (and is often used for) the sharing of information to an

---

[1] ABS Report 8146.0 - Household Use of Information Technology, Australia, 2010-11

[2] ABS Report 1301.0 - Year Book Australia, 2012

[3] ABS Report 8146.0 - Household Use of Information Technology, Australia, 2010-11

audience of their choosing. A person who operates a blog is often seeking as broad an audience as possible. People who share information on social networking sites have varying controls on who can access particular information, and can limit it to particular individuals. However, there is no such desire to broadcast private emails, or a session of internet banking.

The utility in ensuring privacy in the TIA Act is to respect the empowerment that the internet brings to people, and to develop policies which cater for, and does not unnecessarily limit that empowerment, while also giving the community a reasonable expectation that unless they are involved in criminal activities, what they wish to remain private will do so.

Operational Changes

The TIA Act has seen an expansion in the number of agencies which have access to telecommunications interception powers. It has also seen an expansion in the types of agencies using these powers. In addition to ASIO and State and Territory Police, the TIA Act now provides access to telecommunications interception for bodies which target organised crime (such as the New South Wales Crime Commission), anti-corruption agencies (such as the Independent Commission Against Corruption), and Police oversight agencies (such as the Police Integrity Commission).

In addition, the way that Police operate has changed since 1979. There is now a significantly higher level of cooperation, both within an agency, and across agencies (including between jurisdictions) through formal and ad hoc joint operations. Agencies are also in a position to more rapidly react to information that they receive through electronic information management.

The access to, and subsequent use of, information is framed throughout the TIA Act as one agency undertaking one investigation which will lead to a prosecution. The TIA Act needs to be reformed to reflect new operational realities, including the different functions of agencies within the TIA Act, and the fact that effective information sharing is a key component of successful investigations.

Legislative Challenges

The Commonwealth Attorney-General's Department's discussion paper notes challenges which are posed by the current assumptions, drafting and structure of the TIA Act and associated legislation.

One of the key causes of this complexity has been the lack of changes to the fundamental provisions of the TIA Act. As discussed above, the NSW Government believes that the very technological and operational assumptions on which the TIA Act is based are under threat. Therefore, amending the existing legislation will not be enough, as it will likely result in more length and complexity, rather than less.

Identifying Targets

At the time of the TIA Act's drafting, there was a single domestic telecommunications provider, and phone numbers were linked to defined, static locations. It was therefore relatively simple for agencies to link a particular person to a telecommunications service to facilitate an interception. However, this simplicity has been replaced by a de-regulated industry embracing new technology, and targets which have an unprecedented opportunity to avoid detection by law enforcement.

There are now hundreds of telecommunications service providers in Australia. Some are large, and some are very small. The first challenge for law enforcement is to link the person of interest to a service to intercept, or to obtain information about them. Each of these requests requires an authorisation under Chapter 4 of the TIA Act, and there is no guarantee that the authorisation will provide any information.

In addition, while the Integrated Public Number Database provides a starting point to link a phone number with an individual, there is no such system for internet subscriptions.

Once a person has been linked to a service, the agency needs to demonstrate that intercepting that service will provide information in connection with the offence being investigated. Traditionally, agencies will request the records of calls and other communications from the carriers/carriage service provider (C/CSP) providing the service.

Access to this information is vital for both establishing the services being used by a target and their relevant associations. However, equally importantly it represents a strong source of exculpatory information, which can be just as valuable in ensuring agencies are properly targeting their investigations.

However, changes to C/CSPs' business models mean that individual communications are less likely to be billed, so details of these communications are not recorded. The discussion paper raises a data retention regime as a response to this challenge, but does not provide sufficient detail on this proposal.

The NSW Government notes that the Commonwealth Senate Standing Committee on Environment and Communications examined the prospect of a data retention regime in its inquiry into the adequacy of protections for the privacy of Australians online. The Committee raised concerns in relation to this proposal, and recommended that before pursuing such a scheme, the Government should pursue detailed consultation. The NSW Government supports the need for consultation on this important issue.

The proposal will also need to ensure that access to this information is regulated appropriately. The Telecommunications Act 1997 currently provides a number of grounds to access this data either overtly or covertly.

In addition to how C/CSPs operate their businesses, it is now much easier to employ means to avoid detection on Australian telecommunications networks. Individuals can manipulate the identifying features of mobile devices, or purchase mobile devices with modified equipment identifiers which raise significant operational challenges. Despite the criminalisation of this activity, a lack of enforcement provides insufficient deterrent to prevent it. Individuals can also avoid detection by

exploiting identification requirements when purchasing pre-paid telecommunications services, breaking the link between an individual and a service.

More specific operational impediments that are currently being experienced by NSW law enforcement can be canvassed by officers of NSW agencies providing evidence to the Committee.

Identifying Targets – Conclusion

Law enforcement agencies face fundamental challenges in identifying services and persons of interest. These arise from changes to the industry, changes to business practices, and the growing availability of the means to avoid detection.

Applying for a Warrant

Even if agencies are able to overcome the challenges associated with identifying an appropriate target for interception, agencies will face a number of challenges in applying for a warrant to obtain access to those communications, which are set out below.

The NSW Government notes that the Commonwealth is considering merging the warrants for telecommunications interception and stored communications. This would assist in removing duplication during investigations and has a number of other advantages. However, NSW would wish to see the specifics of this proposal, as there are a number of differences in thresholds and safeguards, appropriate controls, oversight and administrative mechanisms that need to be resolved.

This approach will also ensure that there is clarity in relation to whether an issuing authority can issue each of the warrants provided for by the TIA Act, as issuing authorities currently require multiple declarations to be made to issue warrants for telecommunications interception and stored communications respectively.

At the moment, the TIA Act limits the issuing of an interception warrant to the investigation of a 'serious offence', which is defined in section 5D of the TIA Act. Section 5D is an exhaustive list, which is long, complex and unclear. There are a number of specific concerns raised by agencies in NSW.

The lack of a consistent threshold means that some offences for which interception warrants are available are relatively low, but there are also a number of offences with quite significant penalties for which telecommunications interception is not available.

This approach is in contrast to the offences which can be investigated under the Commonwealth and NSW surveillance devices legislation, the Commonwealth Crimes Act, and even access to stored communications warrants in the TIA Act itself, which have more general, penalty-linked tests, with significantly lower penalties than seven years.

As a consequence, a number of serious crimes in NSW cannot be investigated with the assistance of telecommunications interception, including:

- Corruption offences. Many of the offences investigated by the ICAC have a penalty of five years' imprisonment.

Therefore, even though the TIA Act provides for the ICAC to apply for warrants, the TIA Act does not include many of the key offences related to the ICAC's functions.

- Particular public justice offences. Currently, the TIA Act (through subsections 5D(6) and 5D(7)) aims to enable the investigation of offences connected with individuals who assist others to commit offences, and those who provide assistance in avoiding prosecution or disposing of proceeds of the offence.
  However, these descriptors are too narrow to include a number of important offences designed to protect the integrity of the justice system, including:
    - Escape from lawful custody (even if the offender is in custody after committing an offence contained within section 5D);
    - Perverting the course of justice; and
    - Accessory after the fact.
- Offences which sit under subsection 5D(3) of the TIA Act, which require people acting in consort, and other specific conditions. This prohibits warrants being available for the general investigation of serious offences including:
    - Possession of firearms; offences including sexual offences against a person under 16, extortion, dealing in firearms or armaments, firearms trafficking , serious theft or receiving significant stolen property;

Clarity in the TIA Act is vital. It assists agencies to be satisfied that they are applying for and executing a valid warrant and it assists the community to be aware of the conditions that justify an imposition on their civil liberties, and the grounds on which that imposition is justified.

Section 5D shows that relying on a high penalty threshold is an unsuccessful approach to achieving clear parameters for access to powers in the TIA Act. Instead, a lower threshold, such as five years' imprisonment would reduce the number of exceptions we currently see in section 5D, and enable a more considered policy discussion around the merits of including an offence within the regime. It would also remove the descriptors set out in subsection 5D(3), which appear to be in the legislation simply by virtue of the presence in legislation which is becoming increasingly outdated.

However, there are already offences in the TIA Act that do not meet the five year threshold. The NSW Government therefore submits that certain prescribed offences should remain within the TIA Act, noting that, in accordance with section 46(2), the issuing authority would still be required to appropriately consider the seriousness of the conduct requested in the warrant against the invasive nature of the warrant, the amount of related information likely to be collected, the privacy impacts of the operation, and an overall consideration of whether the powers of the warrant are proportionate to the offence being investigated, and the privacy impacts of that investigation.

The NSW Government suggests that a revised TIA Act should include a clearer, simpler test for assessing the offences for which powers under the TIA Act are available. This will be even more

important if the proposal to merge the thresholds for access to telecommunications interception and stored communications goes ahead.

It is also important to ensure that the thresholds for access reflect the escalation of powers available under the TIA Act.

For example, the TIA Act enables intercepted information to be used for the purposes of police disciplinary action. However, if the receipt of this information reveals the suspects of misconduct are in contact with other individuals, the TIA Act does not enable the Police to use an authorisation under Chapter 4 of the TIA Act to obtain the names and key details of those new services.

Notwithstanding the comparison between secondary use and primary access, the different styles of drafting for thresholds to content of communications (which are prescriptive) and access to non-content information (which is purpose-based) can lead to operational barriers for agencies. If it is considered appropriate to make use of intercepted material for a purpose, then the Committee should consider expanding the access to non-content information for similar purposes, to ensure important operations are catered for.

In addition to concerns about the complexity of current thresholds, the process for applying for a warrant can be improved. In particular circumstances, a telecommunications interception warrant can be applied for by way of an application over a telephone. It seems anomalous that legislation which is designed to be technologically neutral limits the application for warrants to telephone applications. NSW submits that it would be highly beneficial for the Committee to consider amendments being made to the TIA Act to specifically allow for urgent applications to be made by email or fax, as well as telephone. This would allow urgent applications in a written form, which would provide greater records of events, and provide operational efficiency.

There are also issues with affidavits associated with urgent applications required under section 51. It requires all officers involved to swear an affidavit within 24 hours of the application. This often results in duplication as the duty officer applying for the warrant is simply relaying information from the relevant investigator. A revised TIA Act should consider avoiding this duplication, and could utilise provisions similar to sections 18, and subsections 17(4) and 17(5) of the *Surveillance Devices Act 2007* (NSW) where a sworn affidavit can be delivered to the judge who issued the warrant within 72 hours, which avoids issues surrounding weekends, absences and other unforseen situations.

The TIA Act should also provide for appropriate mechanisms to do with urgent circumstances. Section 7 of the TIA Act already provides for some emergency situations, however they are limited to occasions where an officer is a party to the communication, or if consent is provided by one party to a communication. These provisions are framed around traditional voice communications where an officer is at one end of a telephone.

The Committee should also consider the limitations that exist in relation to these functions. For example, the TIA Act enables the use of telecommunications data to assist the location of a missing person, but does not enable the use of a prospective authorisation under section 180 of the TIA Act. Prospective authorisations would give a much more responsive and accurate reflection of a missing person's activities.

In the absence of these authorisations, agencies can only look back into the circumstances surrounding a missing person, but need to make ongoing authorisations in respect of what has happened after the person has gone missing. The ability to access live telecommunications data would allow a more timely and effective manner to locate persons reported as missing. The protections which apply in relation to people who chose not to have their new location disclosed should still apply to ensure appropriate respect for that person's privacy.

The Committee should consider how agencies should be able to access communications in times of imminent threat to the life, health or safety of an individual (as is provided for telecommunications data in the *Telecommunications Act 1997*), and what mechanisms should be in place to enable an officer to react quickly to discovering electronic communications linked to serious crime (such as a large scale drug deal, kidnapping or serious assault). Such a scheme would need to incorporate appropriate safeguards and reporting requirements.

Applying for a Warrant – Conclusions

Once a target has been identified, there are still a number of challenges associated with effectively applying for a warrant. The TIA Act is too complex in establishing the grounds for a warrant to be available, and does not adequately provide for the issuing of warrants in urgent circumstances. This leads to delays in the development of warrants and their internal clearance, before consideration by an issuing authority.

Accessing Information Under a Warrant

The above challenges apply even before an attempt to access any communications is made. The combination of legislative and technological challenges means that even if an agency has identified its target, and has successfully obtained a warrant, there are still a number of challenges to overcome to successfully perform an interception.

The TIA Act enables telecommunications interception warrants in relation to a telecommunications service (such as a phone number or email address), or in relation to the devices and services used by a particular person. The TIA Act also requires that an interception must be undertaken with the assistance of a C/CSP.

However, as previously discussed in this submission, the telecommunications industry now extends beyond C/CSPs. These additional providers can operate from offshore (such as overseas email providers), operate websites that enable individuals to communicate, whilst others add features to existing services (such as encryption).

As a result, the C/CSP which receives the warrant may not have any access to, or control of the communications which the agency wishes to target, and may not be able to put in place technical solutions to access the relevant communications. In addition, the agency may be only interested in a handful of these services, but must execute the warrant in relation to a C/CSP, meaning that the person's entire internet subscription is intercepted.

The TIA Act should be amended so that it can facilitate a more targeted interception than in relation to an overall subscriber account. It would also be of assistance to look at other means for

interception, noting that targets can access communications services (such as web mail and social media sites) from any number of locations.

The TIA Act should not provide incentives to criminals to adopt particular services due to outdated legislation. Law enforcement will always face challenges, however the Committee should consider ways to ensure that law enforcement can effectively rely on legislation to lawfully gain access to communications which reveal evidence of serious crimes. In this regard, the Committee should also explore opportunities for remote access to communication devices and the need for law enforcement agencies to be able to effectively respond to issues of encryption and new restrictive technologies.

The NSW Government also supports a more effective enforcement framework, as the current requirement for Federal Court action is too inflexible. The NSW Government also notes the discussion paper proposes changes to the industry assistance framework in the TIA Act. However, the NSW Government further notes that the TIA Act already has the power to make a Determination in relation to standards for interception capability, which has not been made. This could, in the interim, resolve some of the uncertainty around particular obligations.

Accessing Information Under a Warrant – Conclusions

As technology advances and the telecommunications industry continues to diverge and globalise, agencies will no longer be guaranteed access to key evidence for investigations. The TIA Act needs broad based reform to ensure that it accurately reflects technical and operational realities, and ensures that effective oversight and accountability mechanisms are in place to protect privacy.

Interpreting the intercepted material

Even if agencies are able to execute an effective warrant, they still face a number of challenges in interpreting the intercepted information they receive. The intercepted information must be deciphered, and reconstructed into the form that the target of the investigation is using.

When the TIA Act was first enacted, and for a considerable time afterwards, agencies received intercepted material as if they were the intended recipient of the phone call. However, technological change has destroyed this simplicity. Service providers program data passing over networks so that it can be used by the products and systems they provide. Much of this coding is proprietary knowledge, and so agencies face a constant struggle to keep up with new technology so they can make sense of the streams of data they receive.

This is a fundamental issue for any communications passing over a network. Adding to this challenge is the encryption of communications. The NSW Government supports targeted obligations in relation to the decryption of communications that are encrypted, however, further detail about the Commonwealth's proposal for criminal offences is required.

The NSW Government would also suggest that the Committee consider whether the existing interception framework provides the most effective opportunities for agencies to overcome encryption, and whether it should only be addressed through regulatory obligations on the industry.

It should also be enacted in the context of ensuring that encoded communications can also be properly decoded. The NSW Government suggests that this could be addressed in part through

cooperation between agencies. It is therefore vital that the revised TIA Act will not prevent agencies cooperating to ensure they share technical expertise to avoid technical challenges associated with interception.

Interpreting the intercepted material - conclusion

Agencies will face a growing challenge to interpret intercepted information, due to the inherent nature of the modern telecommunications sector, and more widespread and sophisticated encryption of communications. The TIA Act will need to ensure that there are sufficient regulatory and operational mechanisms in place that can respond to this challenge, otherwise agencies will lose a critical capability to investigate crime.

Making Use of the Intercepted Material

The TIA Act places strict controls on the use of intercepted information by the agency which obtains it (through the highly complex, long and regularly amended definition of 'permitted purpose'). In the past, this definition reflected operational processes for police agencies investigating a limited number of investigations prescribed by the TIA Act. However, the more varied nature of agencies operating under the TIA Act, and new processes and procedures for responding to serious and organised crime, have undermined the effectiveness of this approach, resulting in a long and complex series of provisions.

As a consequence, even if an agency overcomes the myriad of challenges it faces in performing an effective interception, it may be hamstrung by the provisions of the TIA Act which manage the flow of information.

For example, there are exhaustive lists in two parts of the TIA Act (sections 5B and 6L) which set out the types of proceedings for which lawfully intercepted information can be used in evidence. While the TIA Act expressly caters for a person's prosecution, other related proceedings, applications for forensic examinations, or proceedings under the *Children and Young Person (Care and Protection) Act 1998*, are at risk of falling outside those definitions, even if they are a direct consequence of the investigation which justified the warrant. There is also ongoing uncertainty as to what happens to lawfully intercepted information once it is in the public domain, such as through transcripts of evidence.

Further, the TIA Act is also silent on other processes that are not 'proceedings', as defined in the TIA Act, including how to record complaints made against officers for misusing intercepted material, and associated disciplinary processes. These limitations can actually limit the options available to the Police Integrity Commission in investigating the misuse of lawfully intercepted information. It is vital that the TIA Act properly empowers agencies to investigate possible misuse of powers in the TIA Act to maintain public confidence in the regime.

NSW broadly supports reducing complexity and improving information sharing provisions. However, the NSW Government would submit that this will be achieved most effectively if the operational, as well as technological changes are considered when redrafting the TIA Act.

With the number of agencies involved in cooperative policing (and the varying purposes for which agencies apply for warrants, including law enforcement, security and oversight of police agencies), a

prescriptive approach will be under constant pressure to properly incorporate all of the necessary elements for effective investigation.

The Committee may wish to investigate whether it is more appropriate to develop a principles-based approach to the management of information, which clearly reflects the policy intent of limiting the use of information obtained under the TIA Act, but facilitating its use in appropriate circumstances.

Principles could include:

- information obtained in the course of an investigation should be available for all stages of that investigation;
- that discovering information relevant to a serious crime, or misconduct of a public officer, should be shared; and
- that discovering information about an impending serious risk to the health, life and safety of individuals should be communicated (e.g. a particular target is armed).

At the same time, there needs to be a limitation on the class of persons or organisations able to receive the material and the use of intercepted information, given its value, and the amount of information to which a warrant can provide access. For example, a general power to combine all intercepted information into a central database for extrapolation is a highly invasive tool. However, particular crime types (such as counter-terrorism investigations) have ongoing relevance to investigations into the future, and so consideration as to how to make use of the operational realities of particular investigations should be incorporated into the legislation.

Clear, concise principles can communicate to the community the grounds on which information can or cannot be exchanged, whilst being sufficiently flexible to avoid the need to legislate for each individual process which arises in each State and Territory.

The Committee should also consider how the prohibitions in the TIA Act interact with the lawful authority of the agencies which use it. For example, there is uncertainty as to whether the prohibitions interact with the powers of interception agencies such as the Police Integrity Commission. There needs to be clarity within the TIA Act, defining with precision when intercepted information may be used to investigate corruption, misbehaviour and misconduct, and when it may be communicated and disseminated to relevant agencies in their oversight capacity, and how the prohibitions in the TIA Act interact with agencies' other powers to request documents (including notices to produce).

The controls in the TIA Act also unintentionally impact on its own efficient operation. For example, subsection 42(4) requires the affidavit to include the number of applications made for warrants and the number of warrants issued in relation to the service or that person. However, this information is protected by the general prohibition on use and disclosure, and so it is very difficult for an investigator to ascertain what other investigations have made applications with regarding the same person or service. Consideration should be given in any redrafted Act to addressing these paradoxes whilst maintaining the appropriate provision of information to the authorities.

Finally, the TIA Act is unclear as to the subsequent use of lawfully shared information. The TIA Act contains a general prohibition on any use or disclosure of intercepted information, subject to the prescriptive exceptions.

This limitation comes from the fact that the power of dissemination in section 68 – the provision that regulates communication of lawfully intercepted information to another agency for its purposes – is limited to the agency that originally obtained that information, referred to as the *originating agency*.

The limitation is most commonly a problem where another agency communicates lawfully intercepted information containing evidence of particular conduct then uses this information to conduct an investigation. If the Police Integrity Commission were to refer evidence obtained from such an investigation (and it contained the originally lawfully intercepted information) to another agency for its purposes (i.e. back to the NSWPF for management action) it is prohibited from doing so as it is not the *originating agency.* In the same way that the TIA Act must provide warrants for key actions of agencies it regulates, the subsequent use of intercepted material by oversight and similar agencies needs to be regulated in a way that facilitates action that can be taken after misconduct investigations, and not just in respect of offences.

Section 68 of the TIA Act enables the Chief Officer to distribute information to another agency for particular purposes. However, section 73 of the TIA Act may limit that agency to distribute the information to any other agencies. The NSW Government is concerned at how these provisions apply to circumstances such as the NSW Police providing information of misconduct to the Police Integrity Commission, and possible unintended limitations on how information is exchanged between those agencies to facilitate an investigation and any action arising as a result of any misconduct identified.

Making Use of the Intercepted Material – Conclusions

There are a number of barriers to effective use of intercepted information in the TIA Act. Definitions such as 'exempt proceeding', 'relevant proceeding', 'proceeding' and 'permitted purpose' provide complexity, which makes it difficult for agencies to properly perform their functions, and makes it difficult for the community to understand the policy rationale of particular provisions.

Record keeping and oversight

The TIA Act contains strict record-keeping and inspection requirements which, among things, require the documentation of each occasion of the use and disclosure of information, and destruction obligations.

For NSW law enforcement agencies, the TIA Act currently separates oversight functions between the Commonwealth Ombudsman and the NSW Ombudsman for stored communications and telecommunications warrants respectively. Given that a number of investigations use both powers, there is an unnecessary overlap of functions. It is recommended that the NSW Ombudsman be empowered to oversee NSW agencies.

One of the other main features of the TIA Act is its attempt to provide oversight and control with highly prescriptive approaches to each process. These processes include requiring that particular processes need to be authorised by sufficiently senior officers.

In describing these roles, there are literally dozens of these terms in the legislation, with corresponding instruments, for questionable policy outcomes. A revised TIA Act needs to deal with this unnecessary complexity, and should look to streamlining the levels of authorisation within the TIA Act to provide clarity for agencies and the community.

The NSW Government would request that the relevant authorisations be reconsidered to ensure effective accountability by vesting responsibilities in officers who have the responsibility to monitor operations. For example, it is impractical to ensure that the Commissioner of the NSW Police certifies that documents have been destroyed. This, for example, may be achieved by revising the definition 'certifying officer' be revised to be at the level of Superintendent (or a public sector equivalent), to more accurately reflect organisational structures in NSW.

It will also be beneficial to ensure that similar processes are overseen by officers of the same level. For example, it would be necessary to ensure consistency between the officers who are authorised under section 55 of the TIA Act to execute warrants, and section 66 which deals with officers who can receive the product of that interception.

Consideration should be given to replacing the requirement to destroy records, with provisions that acknowledge that lawfully obtained information may be required to be lawfully retained for legitimate law enforcement purposes. This is particularly relevant to counter terrorism and organised crime investigations that tend to be protracted. Due to the nature of these crime types, police have found evidence or information from past investigations (including that obtained under the TIA Act) is highly relevant to subsequent investigations, even though such investigations may take place some years later. Experience has also shown that the conviction and incarceration of persons for terrorism or organised related offences does not necessarily diminish their intent or desire to engage in further criminality. It is also noted that, in the consideration of privacy, only minimal lawfully intercepted information is ever placed on the public record.

However, the current requirements which ensure that intrusions are only permitted under carefully controlled circumstances are important elements of the Act, and careful consideration must be given to expand access to this information beyond the scope of that which is available via a warrant. There will also need to be a consideration of effective requirements serving accountability and control purposes.

If consideration is given to expanding or extending the provisions of the Act, these must be accompanied by similar changes to the compliance and inspections requirements to ensure that the accountability and control frameworks continue to be effective and robust.

The NSW Government also notes that there may be benefit in providing officers involved in interceptions a protection against criminal prosecution for activities undertaken in good faith as a course of their activities. As legislative interpretation often occurs after the fact, there should be

clarity that an officer of an agency acting in good faith should not face criminal prosecution for the subsequent decision that activities were not fully compliant with the TIA Act.

Record keeping and oversight – Conclusions

There is no doubt that effective oversight is vital in a revised TIA Act. It will be important that these provisions are clear, effective, and do not overly rely on process-based accountability. The NSW Government looks forward to further advice from the Commonwealth on the detail of its proposals in this area.

Further consultation required

The NSW Government requests that the Commonwealth consult it on the drafting of any amendments to the TIA Act. NSW Government agencies accounted for over half of all telecommunications interception warrant applications in 2010/2011.[4] Accordingly, NSW agencies are key stakeholders. The TIA Act is highly complex and NSW is in an excellent position to provide further input from an operational perspective. Furthermore, given the volume of telecommunications interception warrants in NSW, the TIA Act has a great effect on individuals in NSW.

[4] 1767 out of a total of 3495 (Commonwealth Attorney General, Telecommunications (Interception and Access) Act 1979, Report for the year ending 30 June 2011, at 18)

Chapter 3 – Telecommunications Sector Reform

The NSW Government agrees that as the public and private sector conducts more of its business online, it is important to ensure that we can communicate securely. The discussion paper proposes various regulatory options to provide security. However, as the majority of ICT infrastructure in Australia is owned and operated by the private sector, there needs to be an appropriate balance to avoid excessive regulation.

NSW is concerned at the general nature of the discussion paper, given that it proposes a significant new regulatory impost on the industry, and possibly State Governments. At this stage, NSW would suggest that there is insufficient information contained within the discussion paper to provide complete comments, and would appreciate further consultation before committing to support these proposals, including in relation to any proposed penalties, to ensure that the NSW Government and its law enforcement agencies can continue their positive working relationship with the telecommunications sector.

The NSW Government notes that in other contexts where the private sector are key players in ensuring security, such as regulating chemicals of security concern, Government has generally considered non-binding codes as the best regulatory model, rather than binding regulation. The NSW Government would recommend a more detailed discussion on whether other regulatory options are available.

Another challenge in an enforcement framework is the dynamic nature of the ICT industry, and the rapid rise of threats to particular infrastructure. Regulatory frameworks that require specific action can be susceptible to such an approach, as there is a risk that a previously endorsed action could be subject to new risks that arise in the future. This could be a risk to the Government if it instructs a member of the industry to take a particular course of action, which is followed by that instructed action being victim to exploitation, making the direction redundant, as well as more expensive and restrictive on the industry.

The discussion paper also notes that the cost of compliance will be borne by industry. This could potentially cause prohibitive costs which will discourage investment in the Australian ICT industry. It may also result in costs for States, if ASIO's authority would extend to networks operated by Governments.

If the proposal does apply to State Government networks, the NSW Government would appreciate a full intelligence briefing on the justification for any directions, and ensuring effective information sharing to ensure that any concerns can be addressed as early in the procurement process as possible.

Chapter 4 – Australian Intelligence Community Legislation Reform

The NSW Government notes the small level of detail associated with these proposals. Without more detail, the NSW Government is not in a position to fully assess many of the proposals, and so at this stage, does not feel it is appropriate to develop a position. However, proposals relating to the definition of ASIO staff, ASIO employment arrangements and the disclosure of identities of ASIO officers appear to have little impact for NSW, and so the NSW Government does not express concerns at this stage.

The NSW Government would appreciate further consultation on these proposals. It notes the challenges that ASIO is facing, but feels that there is an opportunity to work together to develop proposals which appropriately balance the solutions with concerns relating to privacy. Ideally, this consultation should occur in relation to policy options, rather than draft legislation, to ensure that States and Territories have adequate opportunities to discuss alternative solutions for the challenges raised by ASIO.

Below are areas of particular concern for the NSW Government.

Create an Authorised Intelligence Operations Scheme

This proposal would allow the Director-General of ASIO to authorise staff, and those assisting ASIO to commit particular acts without civil or criminal liability. The NSW Government would appreciate further consultation on the mechanism that will allow ASIO to undertake activities that would otherwise be in breach of criminal laws, particularly in relation to human sources assisting ASIO, but not being employed by the Organisation. The NSW Government would also appreciate close cooperation between ASIO and its State and Territory law enforcement partners.

If it is considered that ASIO's powers should be the same as a police agency, then consideration needs to be given to binding ASIO to the publicly available oversight which occurs in relation to police agencies.

Clarify ASIO's ability to cooperate with the private sector

The proposed amendment to section 19(1) of the ASIO Act to clarify ASIO's ability to cooperate with the private sector requires further detail. Private sector bodies are not subject to the same accountability mechanisms as public sector bodies. Therefore, any cooperation also ought to be subject to strict controls and transparency requirements.

Furthermore, any cooperation with the private sector ought to be limited in scope. For example, ASIO sharing information with a private organisations relating to security risks is a very different prospect to cooperation in operations.

ASIO powers to enter property

The NSW Government has concerns regarding the proposal that ASIO be given the authority to enter third parties' property when executing a warrant. It is unclear whether the proposal is targeted to third parties relevant to an organisation, or whether it applies to any third party, which owns property close to a target of interest, or in some other way could assist ASIO in executing a warrant.

The NSW Government is concerned that a warrant drafted in this way may give ASIO broad powers to enter the property of an individual with no connection to an investigation beyond their location.

The NSW Government believes that there are options available to provide adequate safeguards, including limiting the proposal to circumstances when notification of third parties cannot occur, and consideration of alternative ways of gaining access.

If such access were permitted, it is arguable that it should be specified in the terms of the warrant (rather than as an incidental power) to ensure oversight and accountability. This would ensure that the issuing officer of the warrant had to cast his or her mind to the appropriateness of the infringement on the third party. Precedent exists at Part 5 Division 4 of the *Law Enforcement (Powers and Responsibilities) Act* NSW

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

Similar to its concerns regarding access to third party property, the use of third party computers raises similar issues about the affect on individuals who may not be relevant to the investigation in question.

The NSW Government agrees with the discussion paper's assessment that accessing third party computers will have privacy implications. Therefore, there needs to be a consideration of whether there are other options available to ASIO to respond to the challenge raised, which can minimise its authority in relation to individuals who are not of interest to ASIO.

In addition, the NSW Government would suggest that it would be beneficial for ASIO to be aware of the computers affected by its operations to ensure proper controls are put in place, or any means available to limit other parties from becoming involved in the operation.

The Committee may also wish to consider whether it would be appropriate for ASIO to be responsible for obligations to either rectify, or compensate for, any damage or disruption caused by such activities.

As with the proposed power to enter third party property, if such access were permitted, it is arguable that it should be specified in the terms of the warrant (rather than as an incidental power) to ensure oversight and accountability.

Definition of computer

In relation to the proposal for a broader definition of computer, the NSW Government notes that it is now much easier to distribute electronic material across a number of computers, and that it may not be apparent until a computer is analysed that important information has been sent elsewhere. As noted in the discussion on the cultural change in the telecommunications landscape, due to the way computers are used by citizens in the 21st century, access to a person's computer without their knowledge is potentially as great an imposition on their right to privacy as the execution of a search warrant on his or her premises. The NSW Government would appreciate further consultation on the proposed changes to the definition of computer, as terms such as 'computer network' are very broad in nature, and can technically apply to large numbers of machines. The refined definition of computer should ensure that it can be appropriately limited to particular circumstances to ensure the warrant still has a limiting affect.

In NSW, under section 75B of the *Law Enforcement (Powers and Responsibilities) Act*, police may search a computer on premises and use that computer to download information from another computer which is not on the premises. This power can however only be exercised on the execution of a warrant and certain safeguards exist in the legislation (eg that the equipment will not be damaged). As with the proposed power to enter third party property, if such access were permitted, it is arguable that it should be specified in the terms of the warrant (rather than as an incidental power) to ensure oversight and accountability.

Enabling warrants to be varied by the Director-General, simplifying the renewal of warrants process and expanding the duration of warrants from 90 days to 6 months

There is no doubt that ASIO should be regulated by efficient processes for gaining an authorisation to discharge its powers. However, this operational efficiency needs to be balanced against the need to ensure that powers are only used in the appropriate circumstances, and are done so with appropriate oversight and accountability.

The discussion paper raises the possibility of extended times for warrants being in force, and suggests that warrants could be varied by the Director-General, and renewed by the Attorney-General. The NSW Government is concerned that there is little detail as to why 90 days is an insufficient time to execute a warrant.

The NSW Government would suggest that enabling the renewal of warrants would also provide an opportunity for the Attorney-General to consider the merits of an ongoing operation, and will provide an opportunity to analyse the outcomes of an operation so far, which may enhance the oversight of ASIO.

The NSW Government is concerned with the proposal that the Director-General would be empowered to vary a warrant issued by the Attorney-General. The NSW Government is concerned as it was the Attorney-General who decided to issue a warrant, and so it is appropriate that the Attorney-General should reconsider matters which have such an impact on an investigation. The NSW Government would be amenable to the proposal in response to operational experience as to why this approach is unworkable.

'Clarification' of Use of Reasonable Force

The discussion paper suggests that provisions of the ASIO Act are unnecessarily limited by the language employed by the headings of those provisions. However, the NSW Government does note that the language of some associated documentation, including the explanatory memoranda for subsection 25(7) in the *Australian Security Intelligence Amendment Legislation Act 1999*, states that subsection 25(7) relates to authorisation of entry methods in relation to the subject premises. The NSW Government is concerned that the Parliament may have intended this limitation, and would be more comfortable with the proposal if operational experience was used to support the proposal.

ASIO Named Person Warrants

The NSW Government is concerned by the proposal of all powers under the ASIO Act being available through one instrument. The discussion paper notes that this proposal should be subject to appropriate accountability mechanisms, however the NSW Government would appreciate further detail on what is considered as appropriate in these circumstances.

The discussion paper does discuss that multiple powers are used in approximately one third of cases, however this does leave the remaining two thirds which do not. The NSW Government suggests that other options, such as streamlining the process for applying for a warrant, or expanding the number of people who can issue warrants for ASIO could be considered to improve the operational outcomes for ASIO, while ensuring that there is still a consideration of the merits of each power, given that they deal with a number of different issues.

NSW considers that a warrant authorising the exercise of multiple powers in respect of a named person would not raise concerns if the issuing authority were satisfied to the requisite threshold of the need for each power. It is doubtful as to whether that approach holds any advantages over the existing approach of seeking multiple warrants.

In addition, there would need to be a mechanism in place to preserve the validity of the warrant, if one component has been ruled invalid. For example, ASIO could be issued a named person warrant, and perform a premises search, use surveillance devices and intercept communications. If the warrant is deemed invalid by the Court in relation to the use of a surveillance device, there would be a risk that the intercept and search of premises would then become invalid also.

Evidentiary Certificates

The NSW Government is concerned at this proposal, as it may limit the opportunity for the legitimate questioning of evidence. The discussion paper raises that Public Interest Immunity, or certificates under the National Security Information (Criminal and Civil Proceedings) Act 2004 are currently available for ASIO, but does not explain why they are not effective, or whether ASIO will continue to rely on them should evidentiary certificates be made available.

The NSW Government is also concerned that there are a number of planned expansions to the ASIO Act in this discussion paper. It may be more appropriate to consider their operation before instituting such a regime. The NSW Government notes that evidentiary certificates under the TIA Act are often used to protect a particular technical capability, or to protect employees of carriers, who provide assistance to law enforcement agencies.

The NSW Government is further concerned at how these amendments would apply to joint operations, as evidence obtained by a law enforcement agency will not be subject to the certificate, whereas evidence obtained by ASIO will be. The NSW Government would appreciate further consultation on the plan to deal with this outcome before such amendments are made.