Submission No 235

Inquiry into potential reforms of National Security Legislation

Organisation: Attorney-General's Department

Parliamentary Joint Committee on Intelligence and Security

Questions on Notice – ASIO Act proposals

1. *Why should ASIO be empowered to hack third party computers that may belong to people who are not threats to national security?*

The proposals would not involve hacking in the sense of authorising ASIO to examine the content of material. AGD notes the concerns raised in submissions to the Committee, for example from the Office of the Victorian Privacy Commissioner, that the proposal would allow surveillance of virtually unlimited services. However, the purpose of a warrant authorising the use of a third party computer would still be to access the computer of security interest, and the warrant would not authorise ASIO to obtain intelligence material from the third party computer or the communication in transit. The use of the third party computer is essentially like using a third party premises to gain access to a the premises to be searched where direct access is not possible. It involves no power to search or conduct surveillance on the third party.

Advances in technology have made it increasingly difficult for ASIO to execute its computer access warrants, particularly where a person of interest is security conscious and may use mechanisms that make it difficult to obtain access to the computer. Therefore, ASIO increasingly has to use innovative methods of achieving access to the computer of interest. In some cases, it may not be possible for ASIO to gain direct access to the relevant computer, and therefore ASIO may be unable to gather vital intelligence important in relation to security. The ability to use a third party computer or communication in transit for the purpose of executing a computer access warrant would enable ASIO to gain access to the relevant computer where direct access is not possible.

There are a range of safeguards that already exist so that third party computers and communications in transit could only be used in limited circumstances. It is envisaged that use of third party computers and communications in transit would need to be expressly authorised by the Attorney-General when issuing a warrant. The Attorney-General's Guidelines contain requirements for ASIO to use as little intrusion into privacy as possible and for the measures used to obtain intelligence to be proportionate to the gravity of the threat (section 10.4).

2. *Why should ASIO be allowed to disrupt a target computer if the law currently prevents that from happening?*

ASIO is currently restricted from doing anything under a computer access warrant that interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be. As this requirement is expressed in absolute terms, it can prevent ASIO from being able to execute a warrant if doing so would have even a minor or inconsequential impact, such as a temporary slowing of the computer. It could also create uncertainty if it is not possible to determine whether doing something under a computer access warrant may interfere with, interrupt or obstruct the lawful use of the computer by other persons.

Allowing the disruption of a target computer, proportionate to what is necessary to execute the warrant, would enable ASIO to continue to access data relevant to security in spite of technological advancements and security conscious investigation targets. It is not intended that ASIO would be able to significantly or materially interfere with lawful use (doing so would be counter-productive as it may enable ASIO's activities to be detected). The proposal is about modifying the limitation so that it is not such an absolute prohibition and permits limited and minor interruptions if necessary to execute the warrant.

3. Why is a 90 day period for the execution of search warrants inadequate?

The ASIO search warrants only authorise a single search of premises. We appreciate that many submissions to the Committee have queried why 90 days is not sufficient time to complete a search. The fact is that in many cases it is possible that a search could be undertaken within 90 days. However, there have been instances where ASIO was unable to execute a search warrant within the 90 day limit for reasons beyond its control. ASIO operations require careful planning, and may require a high degree of flexibility as to when warrants are executed, in order to ensure access to the intelligence information and ensure protection of ASIO officers and methodology. Searches may be undertaken covertly, which may significantly limit opportunities to execute the warrant. A warrant enabling a search to take place within a six month period would provide operational benefits as the exact timing of the search may depend on a range of unknown and fluid operational factors.

AGD notes the Inspector-General of Intelligence and Security's comment that the six month period should be clearly set out as a maximum duration. As with all ASIO warrant powers, six months would be a maximum duration. It would be open to ASIO to apply for a period shorter than six months where appropriate, or for the Attorney-General to grant a warrant with a shorter duration if an adequate supporting case for the maximum duration is not presented.

While it is possible for ASIO to reapply for a new warrant if it has not been possible to conduct the search within the 90 day period, if the search has not been conducted and the grounds remain unchanged, arguably seeking a fresh warrant does not significantly add accountability. The warrant, whether in force for 90 days or six months, still only authorises one search of the premises. There is also a requirement under section 30 of the ASIO Act for the Director-General to notify the Attorney-General and take steps to ensure that any action under the warrant is discontinued if the Director-General ceases to be satisfied that the grounds for it exist.

The proposal to make the duration of search warrants consistent with the duration of other warrants will also assist if the single 'named person warrant' proposal is adopted. It would mean there would be greater consistency among the warrants and the maximum duration for which they can be in force.

4. *What is envisaged for a renewal process for ASIO warrants and how would that differ from applying for fresh warrants?*

Certain threats to security can endure for many years, requiring a significant proportion of warrants issued under the ASIO Act to continue beyond the initial authorisation period. However, the current provisions in the ASIO Act do not specifically enable a warrant to be renewed. In comparison, Ministerial Authorisations under the *Intelligence Services Act 2001* can be renewed and varied.

Applying for a new warrant necessitates restating the intelligence case and completely reassessing the legislative threshold. In accordance with section 28 of the ASIO Act, ASIO must provide the Attorney-General with details of all the facts and grounds on which the Director-General considers it necessary for the warrant to be issued and the grounds on which the Director-General suspects the person to have engaged in activities prejudicial to security.

It is envisaged that a renewal process would differ by enabling ASIO to present a renewal application to the Attorney-General that focuses on why it is necessary to continue the warrant and certifies that the facts and grounds specified in the original application have not changed. A simplified renewal process would provide significant administrative efficiencies for ASIO and the Attorney-General, without reducing oversight and accountability, as the Attorney-General would still need to be satisfied that the application meets the relevant threshold. The ability to renew warrants would streamline the process because the warrant application could rely on the previous case and focus on whether the original grounds for the warrant continue to exist, rather than set out the full case again.

AGD notes the concerns raised by the Gilbert + Tobin Centre of Public Law that the criteria for renewal should not be significantly less than those for issuing a warrant in the first place. The Attorney-General could still have responsibility for renewing warrants, and the IGIS would also continue to have oversight of all warrant documentation. On that basis, the Attorney-General would only grant a renewal if satisfied that the legislative requirements continue to be met. In doing so, the decision to renew warrants would be focused on any change in circumstances from when the original warrant was issued and the appropriateness of continuing the warrant for a further period.

AGD also notes the observation of the Inspector-General of Intelligence and Security that current provisions also require ASIO to provide a report to the Attorney-General on the extent to which each warrant assisted ASIO to carry out its functions. It is not intended to reduce this reporting, and it is envisaged that this proposal would include a similar requirement for ASIO to report to the Attorney-General on the effectiveness of the original warrant in a renewal application.

5. *Which warrants are intended to be varied and in what ways might those warrants be varied? Who would authorise the variation of a warrant?*

Currently, the ASIO Act does not specifically provide for a warrant to be varied. In comparison, Ministerial Authorisations under the *Intelligence Services Act 2011* can be varied.

The proposed variation power might operate in a similar way to the renewal power. It is envisaged that a general power to vary warrants could apply to all warrants under Division 2 Part III of the ASIO Act (this proposal does not cover questioning and detention warrants). A variation might be sought if there is a relatively minor change in circumstances. For example, if ASIO had a computer access warrant relating to a particular computer and also entry to the premises in which that computer is located. If the person moved house unexpectedly, before entry to the premises to access the computer occurred, the ability to request a variation to amend the address could be appropriate, as the core grounds (to access data on the target computer) would not have changed.

The Attorney-General could vary warrants on application by the Director-General, certifying that the original facts still exist, and explaining the necessary changes to the warrant and reasons for this. The ability to vary warrants would streamline processes because the variation application could focus on the changed circumstances rather than have to set out the full case for the warrant application all over again.

Given that the Attorney-General issues warrants and their terms and conditions, it would seem appropriate that the Attorney-General should have the responsibility for approving the variation of warrants. An alternative model that the committee may wish to consider, in relation to the single named person warrant proposal, might be that the Attorney-General issue the warrant, and if appropriate, could include authorisation for the Director-General to vary by adding or removing certain powers (subject to any terms and conditions).

AGD notes the suggestion of the Law Council of Australia that a new warrant should be sought in every instance in which there is a significant change in circumstances. It is envisaged that in instances where there is a significant or material change in circumstances, ASIO would apply for a new warrant, rather than seek a variation.

6. Would ASIO be able to rely on the AFP to conduct controlled operations on behalf of ASIO?

In some circumstances, it is possible for ASIO to utilise the Crimes Act controlled operations scheme, such as where ASIO is involved in joint counter-terrorism investigations with law enforcement agencies. However, reliance on that scheme has significant limitations for ASIO's functions and is not always an option. It is because of the limitations in that scheme that it is proposed to establish a separate scheme for ASIO.

The Crimes Act scheme primarily seeks to regulate the collection of evidence for use in criminal prosecution. The objective of an ASIO authorised intelligence operations scheme would be to protect officers and human sources operating in dangerous contexts to gather intelligence material.

A number of submissions to the inquiry have suggested ASIO should 'task' the AFP to conduct controlled operations on its behalf, rather than relying on a new authorised intelligence operations scheme in the ASIO Act. However, the Crimes Act controlled operations scheme under which the AFP operates was developed in the context of law enforcement, and was not designed for other agencies to 'task' law enforcement to use the scheme for their functions. The controlled operations scheme is for law enforcement purposes and the thresholds and legislative requirements would need to be met by the AFP.

While there might be some capacity to utilise this scheme in joint counter-terrorism investigations, ASIO security intelligence operations extend across the range of national security matters within the ASIO Act. Some operations may cover matters not normally the subject of criminal investigations, such as foreign interference. Similarly, ASIO may be involved at a stage where there would not be sufficient grounds for law enforcement to investigate the possible commission of an offence.

In her submission to the Committee, the Inspector-General of Intelligence and Security acknowledged that there would be operational impediments for ASIO being required to operate under schemes designed for law enforcement agencies, particularly where such schemes emphasise the collection of evidence or are designed for short-term operations. It is envisaged that under an ASIO authorised operations scheme, the Director-General could initially authorise an operation for up to 12 months, reflective of the complex nature of intelligence gathering operations. However, a controlled operation under the Crimes Act initially lasts for three months.

Another limitation with the Crimes Act controlled operations scheme is any involvement by an ASIO officer would be under the direction of a law enforcement officer. This would not allow for existing relationships and contacts by ASIO officers and sources to be maintained during the operation.

In addition, submissions to the Committee have also queried the necessity of an authorised intelligence operations scheme for ASIO, and suggested ASIO rely on prosecutorial discretion. While a general prosecutorial discretion is available, decisions on whether to pursue a prosecution are determined on a case-by-case basis by the relevant Director of Public Prosecutions. It is not normal practice for the Director of Public Prosecutions to give advance indemnities or immunities from future prosecution. In addition, there is no equivalent mechanism to provide indemnity from civil proceedings.

Reliance on prosecutorial discretion does not provide a clear assurance or an effective mechanism for ensuring that ASIO officers or human sources will not be subject to liability for activities undertaken in the performance of ASIO functions.

An authorised intelligence operations scheme could assist ASIO to gain information regarding serious threats to Australia and Australian persons. The need for an authorised operations scheme is to provide assurance to ASIO officers and agents that they have legal protections if it is necessary to engage in certain authorised activities for the purpose of carrying out ASIO's functions in accordance with the ASIO Act. Such a scheme would provide an accountability mechanism to authorise such conduct in appropriate circumstances. Officers and agents would have greater certainty as to what they can and cannot do in an authorised intelligence operation.

7. Why does ASIO need an additional power to be able to enter premises that are not related to the premises of the target person?

Rather than give ASIO an additional power, this proposal seeks to clarify an existing power contained in the search warrant provisions under section 25(4) of the ASIO Act. The warrant may specify that ASIO may do anything that is reasonably incidental to execute a lawfully obtained search warrant, and anything reasonably necessary to conceal the fact that any thing has been done under the warrant.

When executing search warrants, it may occasionally be necessary for ASIO officers to enter third party premises to access or exit the target premises. This may be because there is no other way to gain access – such as where the target premises are in an apartment block and entry is through common areas or adjoining premises – or due to 'emergency' and unforeseen circumstances – such as when the target person unexpectedly returns to the premises during the search.

The incidental power in the warrant provisions is currently relied on where it is necessary to access third party premises. However, it would be preferable to specifically deal with the circumstances that ASIO may be permitted to access third party premises, to provide greater clarity about the detail of the authorisation.

The proposal would simply allow incidental entry to third party premises for the purposes of executing the warrant. It would not provide the power to search, conduct surveillance, or otherwise gather or collect intelligence through the third party premises.

If ASIO knows in advance of the need to gain access via a third party premises, this would be addressed in the warrant application. It is ASIO's practice to approach the owner of the third party premises to seek their consent to access the premises for the purposes of executing the warrant where possible. The proposed amendment is designed to ensure clear legal authority to enter a third party premises in those circumstances where doing so is necessary but where it is not possible to obtain consent to do so, including in an 'emergency' situation where access to third party premises may be necessary to avoid detection.

Some submissions have suggested that ASIO should seek a separate warrant if it needs to access third party premises. However, warrants are issued for the purpose of authorising ASIO to undertake activity to obtain intelligence relevant to security. In this circumstance, ASIO would have no need to obtain intelligence by searching the third party premises, so a separate search warrant would not be a means of granting authority to enter a third party premises to access the target premises.

Finally, we note that the Attorney-General's Guidelines contain requirements of proportionality and using as little intrusion into privacy as possible (clause 10). Therefore, if all ASIO needed to do was access the grounds of a third party premises, it would not do anything more intrusive, such as unnecessarily enter the house.

8. What is the purpose of aligning the surveillance device warrant provisions in the ASIO Act with the Surveillance Devices Act 2004?

Legislation governing ASIO's capabilities with respect to electronic surveillance has not been updated to align with legislation governing the use of electronic surveillance by law enforcement agencies. For example, ASIO's ability to use optical surveillance devices is tied to its ability to use listening devices. This is a relic of the time in which the ASIO Act was first drafted. Additionally, the administrative and procedural provisions governing the use of listening and tracking devices in the ASIO Act are not aligned with provisions governing the use of surveillance devices by law enforcement. Some of the differences where alignment is proposed would be:

- addressing the lack of a separate optical surveillance device warrant
- the provision of a single surveillance device warrant
- the ability to adapt new future technologies by allowing surveillance devices to be prescribed in regulation, and
- clarifying that certain surveillance devices may be used in limited circumstances without a warrant (for example, the use of an optical device that does not involve entry onto premises without permission or interference without permission of any vehicle or thing).

9. What is the purpose in enabling person searches to be undertaken independently of a premises search?

ASIO currently may be authorised to search persons, but only where it has specific authority to do so in a search relating to a premises authorised under section 25. Where ASIO assesses that a particular person may be carrying items of relevance to security, a search warrant relating to a particular premises must be sought. It is only on or near the premises specified in the warrant that a person may be searched.

There have been instances where ASIO has been unable to execute a warrant to search a person as there was no acceptable operational opportunity to do so while the person was on the specified premises. Additionally, if an opportunity to search the person on a separate premises arises, the search cannot take place as the warrant is not linked to that premises. As noted in the Discussion Paper, the sort of scenario where power to search a person might be relevant is where a foreign agent is passing security relevant to material to someone in a public space, such as a park.

The IGIS notes in her proposal that it would be preferable, from an oversight and transparency perspective, to introduce a specific mechanism in the ASIO Act that allows person searches with appropriate limits, rather than relying on premises search warrants to achieve what is effectively a person search in some circumstances. The Committee may have been provided with more detailed classified information about the sorts of circumstances where a person search may be undertaken. The Department or ASIO can expand on this further if required.

The person to be searched would need to be specified in the warrant, and the Attorney-General would need to be satisfied that it is necessary for ASIO to conduct a search of the person to obtain intelligence that is important in relation to a security matter. ASIO would only be able to conduct one search per warrant and could not use the warrant to harass the target at multiple locations. This proposal is not recommending ASIO be given stop and search powers, such as those available to police in some circumstances.

The existing safeguards that apply to searching a person when on a premises would also continue to apply, including:

- Not authorising a strip search or a search of a person's body cavities.
- Where practicable, the search must be carried out by a person of the same sex as the person being searched.
- Key requirements in the ASIO Guidelines that are relevant would be the requirement of proportionality, to use the least intrusive powers where possible, and the need to have regard to the cultural sensitivities, values and mores of certain persons.
- ASIO has internal policies, procedures and training requirements that relate to the proper conduct of searches.
- The exercise of this power, as with all ASIO's powers, would be subject to oversight by the IGIS.

10. Are there any benefits, beyond administrative convenience, in creating a named person warrant that would enable all ASIO powers to be used against a single target?

In approximately one third of cases, more than one ASIO Act warrant type is sought against a particular target. Under the current provisions, this requires the preparation of multiple applications, each re-casting the available intelligence case to emphasise the relevant facts and grounds to satisfy the different legislative requirements of the various warrant types.

The same outcome could be achieved with greater efficiency and with the same accountability by enabling ASIO to apply for a single warrant covering all powers proposed to be used against the target where the relevant legislative thresholds are satisfied. The proposal is intended to cover various warrant powers in Division 2 of Part III other than foreign intelligence collection warrants, and it would not include questioning or questioning and detention warrants.

The use of a named person warrant will increase efficiency in those cases where multiple warrants would otherwise need to be sought. This is more than just administrative convenience, as it is intended to streamline processes to ensure the best use of ASIO's and the Attorney-General's resources without reducing accountability. Arguably, a named person warrant could enhance the Attorney-General's assessment of the appropriateness of the use of particular powers against a single person when issuing a warrant, and whether the use of a particular power or number of powers will assist ASIO in obtaining intelligence relevant to security.

AGD notes concerns raised in submissions to the Committee, for example by the Gilbert + Tobin Centre for Public Law, NSW Council for Civil Liberties, and the Inspector-General of Intelligence and Security, that the single warrant may authorise activities not proportionate to the threat to security. It is important to note that it is not proposed that a named person warrant would provide a blanket authority for ASIO to use any special power. The warrant would need to specify which powers are covered and the use of each power would need to be justified and meet the relevant legislative threshold. It is not intended that this proposal will weaken any of the thresholds.

11. In what circumstances is it envisaged that that reasonable force may be used during the execution of a warrant?

A number of the ASIO warrant provisions provide that ASIO may be authorised to 'use any force that is necessary and reasonable to do the things specified in the warrant' (subsections 25(7), 25A(5A), 26B(4) and 26C(4)). These provisions are found under headings relating to 'authorisation of entry measures'. In light of changes made in 2011 to section 13 of the *Acts Interpretation Act 1901* (Cth), the headings form part of the ASIO Act. However, the terms of the use of force provision are not stated so as to limit the use of force to enter the premises. At the time these subsections were inserted into the ASIO Act, in 1999 and 2005, there does not appear to have been an intention to limit the use of force to entry, as headings were specifically excluded from the Act at that time.[1]

In addition to the possible need to use force to enter a premises, it may be necessary to use force to obtain access to a locked room or locked cabinet, or to use force to install or remove a surveillance device. The proposal is intended to ensure the power to use any force that is necessary and reasonable to do the things specified in a warrant is not read down by reference to the heading and limited to entry.

The existing provision requires that the use of force must be reasonable and necessary to do what is required to execute the warrant. The ASIO Guidelines requirement of proportionality and using as little intrusion into privacy as necessary are also relevant safeguards in this context.

[1] Subsections 25(7), 26B(4) and 26C(4) inserted in the ASIO Act under the *Australian Security Intelligence Organisation Legislation Amendment Act 1999* (Cth) and subsection 25A(5A) inserted by the *Anti-Terrorism Act (No. 2) 2005* (Cth).

Parliamentary Joint Committee on Intelligence and Security

Questions on Notice – TIA Act proposals

1. What is AGD's view on what record keeping arrangements there should be for the TIA Act?

Record keeping and accountability obligations require law enforcement agencies to keep records relating to documents associated with warrants issued and particulars relating to warrant applications (such as whether an application was granted or refused) and each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed. Agency heads must also report to the Attorney-General on the use and communication of intercepted information within three months of a warrant ceasing to be in effect. The Attorney-General's Department must prepare an annual statistical report about the use of powers under the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), which the Attorney-General tables in Parliament.

Different record keeping requirements apply to stored communications.

The requirements are aimed at ensuring that agencies keep appropriate records necessary to demonstrate that agencies are using their powers lawfully. However, many of the requirements reflect ad hoc accumulation of requirements and do not reflect the current governance and accountability frameworks within which agencies operate.

Discussions between agencies and issuing authorities have indicated that new record keeping and reporting requirements are needed that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion into privacy under the regime is proportionate to the public outcome obtained.

2. What is AGD's view on changing the Commonwealth Ombudsman's oversight arrangements? What is the rationale for this view?

Greater consistency in Commonwealth/State inspections

As stated in the Department's Discussion Paper (at page 26), oversight of law enforcement agencies' use of interception powers is split between the Commonwealth Ombudsman and equivalent State bodies. The Commonwealth Ombudsman inspects the records of both Commonwealth and State agencies in relation to stored communications. This split in responsibility contrasts with the *Surveillance Devices Act 2004*, where the Commonwealth Ombudsman inspects all agencies.

While there is an argument for the Commonwealth Ombudsman to oversight every Commonwealth, State and Territory agency's use of powers under the TIA Act, the Department is of the view that it would be more efficient and cost effective to maintain the current split between Commonwealth and State oversight agencies and to extend this to provide that State and Territory Ombudsman, or the equivalent State oversight agency, exclusively oversights State and Territory agencies. The Commonwealth Ombudsman would continue to have responsibility for oversighting Commonwealth agencies.

This approach would avoid potential complexities created by having the Commonwealth Ombudsman oversight the use of an investigative power by State law enforcement agencies for the purposes of investigating State offences.

While the Department considers that State and Territory oversight agencies have a clear role in undertaking audit oversight activities of State and Territory agencies' use of powers under the TIA Act, there is limited ability for the Commonwealth to intervene in circumstances where there are concerns in relation to a State or Territory agency exercising these powers. The Commonwealth must rely on State oversight or a matter may be referred to the Australian Federal Police in extreme circumstances. As the Commonwealth is ultimately responsible for the use of these powers, the Department considers that there is merit in providing that the Attorney-General may task the Commonwealth Ombudsman to undertake an inquiry into a State agency's exercise of powers under the TIA Act where concerns have been raised.

Page 9 of the Attorney-General's Department submission states:

"The diverse range of agencies that can access data and the degree of data generated by the IP world in particular suggests that consideration could be given to distinguishing between data types so as to allow certain agencies access to less descriptive forms of data while restricting access to more detailed data types."

3. How would AGD envisage the distinction between data types, and what is the rationale for the distinction?

Currently, the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) distinguishes between access to existing telecommunications data (referred to as 'historic' data and accessed under the TIA Act) and telecommunications data that comes into existence in the future (referred to as 'prospective' data and accessed under the TIA Act). The TIA Act does not distinguish further between categories of telecommunications data.

The Department's working definition of 'telecommunications data' includes two categories of data:

- information that allows the communication to occur – referred to as 'traffic data', and
- information about the parties to the communications – referred to as 'account-holder data'.

The rationale for the distinction between these types of data is to more closely align the categories of telecommunications data with the sensitivity of the telecommunications data. Creating a distinction between data types would allow greater granularity in the agencies which may access the data types.

4. Which agencies does AGD consider should be removed from, or have limited access to, the access to communications regime?

Real-time content based warrants are only available to 16 Commonwealth, State and Territory law enforcement agencies. Telecommunications data is available both to these 16 agencies and 'enforcement' agencies. Under the TIA Act enforcement agencies can authorise the disclosure of telecommunications data for the enforcement of criminal laws, laws imposing a pecuniary penalty and for the protection of the public revenue.

In practical terms, this allows a wide range of Commonwealth, State and Territory regulatory bodies to access both traffic and account holder telecommunications data for these purposes. These bodies include the Australian Customs and Border Protection Service, the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, the Australian Taxation Office, Centrelink and a range of State and Territory government organisations such as Government Departments and Shire Councils.

As communications technology and use has changed, some data types have become more privacy intrusive. Access to the more privacy intrusive 'traffic data' could then be limited to those agencies that have a demonstrated need to access this information for undertaking their investigative functions. The less privacy intrusive category of 'account-holder data' would be available to the broader range of enforcement agencies.

5. In what way does AGD think the information-sharing provisions [sic] be simplified?

The use and disclosure of information obtained from exercising powers under the TIA Act is strictly regulated. Further, the ways in which information can lawfully be used depends on whether the information was obtained under an interception warrant, a stored communications warrant or data authorisation.

Generally information can be used by the agency that obtained the information for the investigation of a 'serious offence', including the offence listed on the warrant, or the investigation of any offence with a maximum of at least three years imprisonment.

Separately, the TIA Act prescribes the circumstances in which an agency which intercepted information can disclose that information to another agency for use in the receiving agency's investigations. The prescriptive sections limit both the agencies which can receive information and the circumstances applicable to each of those agencies.

These two mechanisms operate independently. For example, the Australian Federal Police may use the first limb to share intercepted information with the Australian Securities and Investments Commission (ASIC) when jointly undertaking an investigation. This is permitted because the sharing is for the investigation of a serious offence and to specific officers who are participating in the joint investigation. However, ASIC cannot use this information more broadly for its own purposes because the sharing did not occur under the disclosure provisions. Use by ASIC is prohibited even if ASIC intends to use the information to investigate an offence with an imprisonment period of more than three years.

A number of issues are caused by the disclosure provisions proscriptively listing both the circumstances required and the agencies which can receive information. For instance, when an agency is granted a new function, amendments to the TIA Act are required to allow that agency to receive information for that function. Similarly, if a new agency is added to the regime amendments are required to specify that the agency can receive information, and the specific circumstances in which it can receive information.

The Department supports the harmonisation of the rules for dealing with information and those dealing with 'internal use' and 'disclosure to other agencies', including where the information is disclosed for the purposes of furthering the disclosing agencies investigation and allowing the receiving agency to use it for furthering their own investigations so that rules are based on the type of the information, rather than the method of access. Applying a single rule to both use and disclosure would be simpler than the status-quo and avoid the current situation where agencies are required to second staff or conduct joint investigations in order to gain the necessary cross-agency expertise needed for particular investigations.

6. Can AGD provide examples of legislative duplication within the TIA Act?

As discussed on page 17 of the Department's Discussion Paper, the pace of change over the past ten years in the telecommunications environment has required frequent amendments to the TIA Act which have resulted in duplication and complexity that makes the legislation difficult to navigate, interpret and comply with.

Key areas of duplication relate to the different types of warrants, including the distinction made between intercepted and stored communications. As stated in the Department's submission (pp3-5) the Department considers that the multiple types of warrants under the TIA Act are duplicative and no longer appropriate for the modern communications landscape.

The oversight, record keeping and reporting provisions which flow from these warrant provisions are also duplicative. For example, in relation to oversight responsibilities, there is dual oversight of State and Territory agencies by both the Commonwealth Ombudsman and the relevant State or Territory oversight agency as discussed in the response to question on notice two above.

In relation to record keeping and reporting, there are three separate annual report requirements for telecommunications interception warrants, stored communication warrants and access to telecommunications data. In the case of interception warrants there are separate annual report requirements for Commonwealth agencies and State prescribed authorities, there are also two separate reporting requirements for State agencies. The three requirements differ making it difficult to undertake a meaningful analysis and comparison of the different mechanisms.

The Department considers that streamlining and modernising lawful access to telecommunications provisions through the creation of a one warrant regime that regulates access to the content of a communication, together with the flow on effects to the oversight, record keeping and reporting requirements, will remove significant duplication and complexity from the TIA Act and create consistency in the accountability framework.

7. In what way could the cost sharing framework be amended to 'align industry interception assistance with industry regulatory policy'?

Consistent with the Government's commitment to reduce the burden of government regulation, the Department believes changes could be made to the telecommunications interception regime to provide clearer regulation for telecommunication service providers, identify clear regulatory offsets and provide a more flexible approach in its application to a diverse global telecommunications environment.

As stated in the Department's Discussion Paper (pp27-28) and Submission (pp5-7) to the Inquiry, the Department sees value in modernising the telecommunications assistance regime to:

- extend assistance obligations to the wider range of current telecommunications industry participants providing services in Australia, and
- acknowledge that a 'one size fits all' regulatory regime does not always equate to a 'level playing field' within a diverse industry.

Current cost allocation framework

As part of carrier licence conditions or service provider rules, Carriers and Carriage Service Providers (C/CSPs) are required to meet their obligations under Chapter 5 of the TIA Act which relates to developing, installing and maintaining interception and delivery capabilities.

The TIA Act provides that C/CSPs are responsible for the cost of developing, installing and maintaining interception capability. The TIA Act also provides that, while C/CSPs initially bear the cost of developing, installing and maintaining delivery capability, C/CSPs can recover these costs over time from agencies.

In effect, C/CSPs are responsible for interception capability costs, while agencies are responsible for the costs of delivery capability.

The *Telecommunications Act 1997* (Telecommunications Act) also has cost allocation principles that apply to the cost of providing reasonably necessary assistance. The principle for these costs is that C/CSPs should provide them on the basis that they neither profit from, nor bear the costs of providing the assistance. The Telecommunications Act also provides that C/CSPs and agencies may create contractual arrangements governing the terms and conditions on which reasonably necessary assistance must be provided.

This reflects established funding and cost responsibility principles for the maintenance of effective telecommunications interception capabilities initially established following the 1994 review by Mr Pat Barrett into the *Long term Cost-effectiveness of Telecommunications Interception* (Barrett Review) and subsequent amendments to the cost sharing arrangements in the Telecommunications Act (now incorporated into the TIA Act). The requirement for all industry participants to have the same interception capability can also be an expensive and unnecessary burden that can act as a barrier to entry to the telecommunications market for new industry players. Therefore, requiring all service providers to have the same interception capability regardless of size (as in the current system) could have the effect of restricting competition rather than promoting it and stifling innovation (noting that the promotion of the supply of diverse and innovative carriage services and content services is one of the objects of the Telecommunications Act).

The current industry and legislative cost allocation framework is working well, but efficiencies may be able to be made in regards to standardisation of technical and administrative requirements in meeting these obligations. Opportunities for reducing red tape and achieving regulatory offsets may also be identified.

Parliamentary Joint Committee on Intelligence and Security

Questions on Notice taken at hearing on 2 November 2012

Senator Faulkner asked the following question at the hearing on 2 November 2012:

Senator FAULKNER: All right, two documents were handed to them. Were they developed in the Attorney-General's Department exclusively, or were other agencies—law enforcement, security or intelligence agencies—involved in the development of those documents?
Ms Smith: Other agencies were involved in the development of those documents.
Senator FAULKNER: That work preceded the round table or consultation processes you had with industry participants, one assumes.
Ms Smith: Yes.
Senator FAULKNER: When did that start?
Ms Smith: I cannot recall when it actually started—
Senator FAULKNER: Could you take that on notice for the committee, please.
Ms Smith: I can certainly take that on notice.

The answer to the honourable senator's question is as follows:

The work that preceded the consultation process undertaken by the Department with Industry Participants began on 1 October 2008.

The Hon Anthony Byrne MP, Chair, asked the following question at the hearing on 2 November 2012:

CHAIR: Another thing I would ask you to contemplate—and I flagged it at the start of my discussion with you—is some additional privacy protection. Notwithstanding that we could be clarifying the points that Senator Brandis and Senator Faulkner have made, I would like you to contemplate what mechanism could be used to safeguard privacy on the use of this database—the metadata—because it has been put to me by telcos that one of the concerns that they have is that you are basically creating almost a honeypot of information. If you segregate that information out of the data that telecommunications companies basically accumulate each day, it would create an incentive for people to try to access that. I would ask you to contemplate what form of mechanism or person or structure could be used to ensure that there would be greater privacy protections if this regime is implemented.
Mr Wilkins: We will do that.
CHAIR: You can take that on notice and put that to us in writing.

The answer to the honourable member's question is as follows:

Telecommunications data, including personal information such as subscriber details, is already collected and retained by industry. National Privacy Principle 4 requires that organisations take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. If there is a breach in the security and data is unlawfully accessed, the unlawful access may be an offence under the Criminal Code Act 1995.

Additionally, the proposed Telecommunications Sector Security Reforms also under consideration by the Committee are based on the introduction of a universal obligation for providers to protect their networks

and facilities from unauthorised access by ensuring competent supervision and effective control over infrastructure and data held on it and transmitted across it.

Under the Privacy Act 1988, agencies and organisations are subject to requirements to provide adequate security protection for personal information in their possession. These obligations will be retained under proposed reforms to the Privacy Act, contained in the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, which will enhance the powers of the Information Commissioner to enforce these requirements will be strengthened. For example, the Commissioner will be able to seek civil penalties against companies who commit serious or repeated interferences with privacy.

Further, on 17 October 2012, the Attorney-General released a Discussion Paper entitled Australian Privacy Breach Notification which has sought views by 23 November 2012 on the possible introduction of mandatory data breach notification laws. Although many companies voluntarily report data breaches to the Office of the Australian Information Commissioner (OAIC), there is no requirement under the Privacy Act to notify the OAIC or any other individual in the event of a data breach. If enacted, mandatory data breach notification laws could complement the current legislative security requirements and a data retention regime in a least four ways by: (1) mitigating the consequences of a breach; (2) creating incentives to improve security; (3) tracking incidents and providing information in the public interest; and (4) maintaining community confidence in legislative privacy laws. The Government is currently considering responses to the discussion paper.

Offences for misuse of data

In addition to the *Privacy Act 1988*, there are a comprehensive range of offences contained in Commonwealth legislation with regard to the potential misuse of stored telecommunications data, the current provisions of the above Acts are relevant in the following circumstances:

- Misuse of telecommunications data obtained by Australian agencies under data authorisations falls under the *Telecommunications (Interception and Access) Act 1979*;
- Misuse of telecommunications data by employees of telecommunications industry providers, emergency call persons and number database persons falls under the *Telecommunications Act 1997*;
- Unauthorised access to telecommunications data over telecommunications networks and/or computers falls under the *Criminal Code Act 1995*; and

Additionally, secrecy obligations will also arise from employment by employees who deal with telecommunications data. Further details of these current offences are provided at **Attachment A**.

Details of current offences for misuse of data (in the context of a data retention scheme)

The *Telecommunications (Interception and Access) Act 1979:*

Section 182 of this Act provides that it is an offence to further use or disclose data originally obtained by agencies for a purpose different to that which was originally authorised (known as 'secondary use/disclosure offences'). There are exceptions to the offence under section 182 where that use or disclosure is for the purposes of enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue. The section carries a penalty of 2 years' imprisonment.

Other than the secondary use/disclosure data offences, the offences for the misuse of telecommunications data generally are not expressly found in this Act. However, section 7(1) of the Act provides the offence for the interception of communications passing over a telecommunications network. In addition, section 63 prohibits dealing with intercepted information. These offences under sections 7(1) and 63 are subject to the warrant, emergency and exemption provisions found in Chapter 2 of the Act for the law use or disclosure of such information. Section 105 of the Act provides that contravention of sections 7(1) or 63 is punishable by imprisonment for 2 years.

Similarly, the Act provides offences for accessing stored communications under section 108, and prohibitions on dealing with accessed stored communications under section 133. These offences are also subject to the lawful use or disclosure exemptions contained within Chapter 3 of that Act. Both offences carry a penalty of 2 years' imprisonment or 120 penalty units or both, as provided for under those respective sections.

The Act also provides for civil remedies for interception of communications in contravention of section 7(1) under Part 2-10 of the Act (sections 107A-107F), or for access to stored communications in contravention of section 108(1) under Part 3-7 of the Act (section 165-170).

The *Telecommunications Act 1997:*

While the *Telecommunications (Interception and Access) Act 1979* provides offences for the secondary use/disclosure of data obtained via agency authorisations under that Act, the *Telecommunications Act 1997* provides offences for the use/disclosure of this data by telecommunications industry providers.

Sections 276, 277 and 278 of the Act provide primary use/disclosure offences for the misuse of telecommunications information held by employees and contractors of carriers/carriage service providers, number-database persons and emergency call persons respectively. These offences apply to unlawful use/disclosure of both '*the content or substance of a communication*' and *'the affairs or personal particulars*' of other persons. These offences carry a penalty of 2 years' imprisonment. The Act provides a number of exceptions to these offences where the person is acting in the course of their duties, as authorised by law, or in an emergency, in addition to particular exceptions listed in Division 3 of Part 13 of the Act.

The Act also provides for secondary use/disclosure offences under Division 4 of Part 13, which apply to the above persons who have been given telecommunications information in the course of their duties. In a similar manner to the prohibitions referred to above, there are exceptions for use authorised by law in addition to particular exceptions listed under that Division.

The *Criminal Code Act 1995*:

Part 10.6 of the Code contains provisions relating to telecommunications services. Division 474 lists a range of offences which may be carried out over a telecommunications network, with the penalties for most of these offences ranging from one to 5 years, including:

- 474.2 Dishonestly obtaining a gain from a carriage service provider by way of the supply of a carriage service;
- 474.4 Manufacturing, advertising, selling or being in possession of an interception device;
- 474.5 Causing the wrongful delivery of communications;
- 474.6 Interference with facilities owned by carriers, carriage service providers and nominated carriers;
- 474.7 Modification etc. of a telecommunications device identifier;
- 474.8 Possession or control of data or a device with intent to modify a telecommunications device identifier;
- 474.9 Producing, supplying or obtaining data or a device with intent to modify a telecommunications device identifier;
- 474.10 Copying subscription-specific secure data from account identifiers;
- 474.11 Possession or control of data or a device with intent to copy an account identifier;
- 474.12 Producing, supplying or obtaining data or a device with intent to copy an account identifier;
- 474.14 Using a telecommunications network with the intention to commit a serious offence

The majority of the offences under Division 474 of the Code contain a defence for law enforcement officers, intelligence officers or security officers where these officers are acting in good faith in the course of their duties and the conduct of the officer is reasonable in the circumstances for the purpose of performing those duties. Similar good faith exceptions to these offences apply to emergency service and National Relay Service personnel under section 475.1A of the Code. Section 10.5 of the Code also provides a general exception to any offence in the Code if the conduct constituting the offence is justified or excused by or under a law.

Similarly, Part 10.7 of the Code contains provisions relating to computer offences. Section 477.1(1) creates the offence of causing unauthorised access to or modification of data, or impairment of electronic communications, with an intent to commit a serious offence (a Commonwealth, State or Territory offence that is punishable by imprisonment for a period of 5 or more years). In order for this offence to be established, the unauthorised access, modification or impairment must be caused by means of a carriage service. This offence attracts a maximum penalty not exceeding the penalty applicable to the serious offence intended. Exceptions to these offences for law enforcement officers are found under section 476.2 of the Act: these exceptions apply where the unauthorised access, modification or impairment is carried out under a warrant issued under the law of the Commonwealth, a State or Territory, or an emergency

authorisation given to the law enforcement officer under the provisions of the *Surveillance Devices Act 2004* (Cth) or a State or Territory law of similar effect.

Divisions 477 and 478 also provide further offences relating to the unauthorised access, modification or impairment of data or communications that apply to conduct involving Commonwealth computers or data and/or a carriage service. The penalties for these offences vary from 2 to 10 years' imprisonment.

The *Privacy Act 1988*:

Misuse of telecommunications data may also fall under the provisions of the *Privacy Act 1988*. The Information Privacy Principles (IPPs) are found in Division 2 of Part III of the Act, and apply to Commonwealth agencies (with the exception of national security agencies). The National Privacy Principles (NPPs) apply to organisations and are found in Schedule 3 to the Act. Organisations generally are private sector bodies such as corporations. A number of bodies, including small businesses are not treated as organisations.

Part IIIAA of the Act governs the use of approved privacy codes, which organisations may develop and submit to the Information Commissioner for approval.

These privacy principles in the Act apply to ***personal information***, which is defined in the Act as being *information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion*.

Both the IPPs and NPPs govern the collection, storage, use and disclosure of personal information and include the following principles relevant to the misuse of telecommunications data:

- The collection of the personal information must be lawful, for a lawful purpose, and must not be obtained by unfair or intrusive means;
- The personal information must protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
- A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record is accurate, up to date and not misleading; and
- A record-keeper who has possession or control of a record that contains personal information shall not use that information for a secondary purpose, or disclose the information unless certain exceptions apply (eg where the person has consented to the release of their personal information, or where the use or disclosure of that information is required or authorised by or under law).

Division 1 of Part III of the Act provides that an interference with privacy occurs where there is a breach of the IPPs, NPPs or an approved privacy code.

The Information Commissioner has powers of investigation of privacy breaches under the Act after receiving a complaint or on the Commissioner's own initiative. After the investigation of a complaint, the Commissioner may make a determination in regards to whether a breach of privacy has occurred. Section 52 of the Act provides that these determinations may:

- Declare that a breach of privacy has occurred, and that the respondent should not repeat or continue such conduct; and

- Declare that the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant.

Respondent organisations must comply with these terms of the determination under section 55 of the Act. The declaration may also find the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint.

These determinations may also be referred to the Federal court or Federal Magistrates Court for enforcement under Division 3 of Part V of the Act. The courts are entitled to issue declarations of right and injunctions in that regard, or may conduct a hearing *de novo* on the question of whether the respondent has breached the privacy of the complainant and make the appropriate orders accordingly.

Secrecy provisions arising from employment

In addition to the legislative provisions which may apply to misuse of telecommunications data above, employees who deal with telecommunications data may be under an express or implied obligation by their employer to deal with telecommunications data appropriately. If an employee misuses telecommunications data, their employers may also face a common law action under the tort of negligence as a result of the employer's vicarious liability for the actions of its employees.

Similarly, telecommunications sub-contractors or agents may also be bound by the terms of their engagement with their principal in regards to the use of the telecommunications data held by the principal. These terms of engagement may attempt to define the terms of liability for any misuse of data in addition to common law agency principle