Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010

1.1 Overview

The Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 (the Bill) was introduced into the previous Parliament on 24 June 2010 and lapsed when Parliament was prorogued on 19 July 2010.

The Bill was re-introduced unchanged on 30 September 2010. The main purpose of the Bill is to amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) and the *Intelligence Services Act* (the IS Act) to enable greater cooperation, assistance and information sharing within Australia's law enforcement and national security communities. The Bill continues the Government's focus on harnessing resources in support of whole-of-government law enforcement and national security priorities and responding to the modern security environment and emergence of new challenges as a result of advances in technology.

1.2 Cooperation and information sharing for law enforcement and intelligence agencies

1.2.1 Assistance to law enforcement with telecommunications interception

Interception agencies face challenges from rapid technological changes that impact on their ability to gain lawful access to highly valuable evidence through telecommunications interception. In this light, it is necessary to ensure the effective and efficient use of technical resources on a whole-of-government basis to overcome challenges where appropriate.

The TIA Act currently allows law enforcement agencies to approve officers or classes of officers of another interception agency to exercise the authority conferred by a telecommunications interception warrant. However, this authority does not currently extend to relevant officers or employees of the Australian Security Intelligence Organisation (ASIO).

ASIO has expertise in a number of areas that would assist law enforcement agencies to exercise the authority conferred by a telecommunications interception warrant. The Bill aims to efficiently utilise resources by enabling a law enforcement agency to seek assistance from ASIO when exercising a telecommunications interception warrant.

This amendment will assist agencies to stay up to date with technological advancements and provide greater support to whole-of-government efforts to protect our communities. Where an officer or employee of ASIO assists a law enforcement agency, the Bill makes associated amendments for the notification to carrier and carrier service providers of a warrant being issued, the revocation of warrants and the issuing of evidentiary certificates about things done through those warrants. The Bill will require ASIO to provide the necessary information to enable the law enforcement agency to comply with its recordkeeping and reporting obligations for the publically available annual report and for records subject to inspection by the Ombudsman.

These amendments will not expand the circumstances in which law enforcement agencies are able to apply for interception warrants or the type of information that law enforcement agencies are currently able to access under the authority of the warrant. ASIO will not be able to use intercept information for its own purposes. Information obtained under an

interception warrant will remain subject to existing safeguards that maintain the integrity of the interception regime including limitations of use, disclosure, recordkeeping and reporting requirements.

1.2.2 Improving cooperation and assistance between intelligence agencies

As recognised in the 2008 National Security Statement, modern national security challenges are increasingly complex and inter-connected. The Smith Review, the National Security Statement and the Counter-Terrorism White Paper all highlighted the importance of increased interoperability and intelligence sharing among the national security community. An integrated intelligence community is essential to Australia's ability to respond to modern national security challenges.

The existing legislative framework places some limitations on the ability of security and intelligence agencies to cooperate. The agencies are only able to cooperate with other agencies where this is necessary or conducive to their own specific functions. This can prevent cooperation in support of whole-of-government national security priorities from occurring to its fullest extent. For example, in a multi-agency team environment that has a role of producing intelligence assessments, the agencies that do not have assessment functions may be limited in the extent of the contribution that they can make to the work of that multi-agency team.

The amendments will enable ASIO, the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO) to assist with the performance of one another's functions. The amendments will enable agencies to make staff and other resources available to multi-agency teams and to assist other agencies carry out their functions. It will ensure that expertise available in specific agencies can be utilised for the benefit of the intelligence community.

It will also be possible to prescribe other agencies by Regulation for the purpose of enabling ASIO, ASIS, DSD and DIGO to cooperate with and assist other Australian Government bodies in the future, should this be considered desirable. The Government does not currently have any intention to prescribe other agencies for this purpose. However, given increased interoperability is a feature among the broader national security community, it may be desirable to extend cooperative arrangements to other agencies in the future.

To maintain independence of the agencies, the Heads of the relevant security and intelligence agencies will be responsible for determining when cooperation or assistance will be provided under these provisions. Agency Heads may agree to requirements, restrictions or limitations to ensure appropriate monitoring of such arrangements at an agency level. The agencies will also need to comply with any relevant Ministerial directions or arrangements. These measures supplement the existing oversight of the agencies by the Inspector-General of Intelligence and Security (IGIS), which is an independent statutory office responsible for oversight of Australia's intelligence agencies. Consistent with its current role, the IGIS will be able to monitor cooperation and assistance provided under these provisions to ensure that each agency acts legally and with propriety and complies with ministerial guidelines and directives.

1.2.3 Enhancing the communication and sharing of intelligence between agencies

The Bill provides greater flexibility for ASIO to share information obtained in the performance of its functions with other Australian intelligence agencies and the broader national security community.

The Bill amends the communication provisions in the ASIO Act to further support intelligence sharing between ASIO, ASIS, DSD, and DIGO if the information relates, or appears to relate, to the functions of those agencies.

The amendments also remove the strict limitation that security information must be communicated for purposes relevant to security 'and not otherwise'. This removes ambiguity that could arise if another provision were to purport to authorise ASIO to communicate security information for purposes other than security, but not specifically state that it overrides the requirement 'and not otherwise'. This amendment does not in itself provide authority to communicate security information for non-security purposes.

The amendments also provide greater flexibility for ASIO to communicate information relevant to a serious crime or where the national interest requires, to the most appropriate Minister, Commonwealth or State authority. Currently, ASIO may only provide such information to a list of entities specified in the legislation. This approach does not adequately provide for the possibility of new agencies being created or changes to the responsibilities of agencies within Government. This amendment will ensure that information is able to be provided to the most appropriate body, having regard to the nature of the information and the functions of that body. The Bill also addresses a limitation in the current provisions such that ASIO can only communicate information about matters in the national interest if that information was obtained by ASIO outside Australia or concerns matters outside Australia. The Bill will provide that ASIO may communicate all relevant information where the national interest requires it.

The amendments relating to cooperation, assistance and communication were developed in close consultation with the interception, security and intelligence agencies and relevant departments. Other members of the national security community and the IGIS were also consulted.

1.3 Access to telecommunications information

1.3.1 Missing persons

Locating missing persons is an important priority for law enforcement agencies with around 35,000 people reported missing in Australia each year. While the Government and Police Forces are aware that many missing persons have gone missing of their own volition, many of the missing persons have gone missing as victims of unlawful activity.

Telecommunications data is information about the process of a communication as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details collected by the C/CSP to establish details about a communication.

The TIA Act currently enables authorised agencies to access telecommunications data for the purposes of security, the enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue. However the TIA Act does

not currently provide for circumstances where police are performing functions in relation to protecting public safety short of investigating unlawful conduct, including locating missing persons.

Access to telecommunications data for the purpose of locating missing persons will provide valuable leads about where a missing person might be and who might be able to provide information about that missing person. Telecommunications data can provide information such as call records and in certain circumstances provide location information to establish patterns about a person's movements as well as signs of life.

The Bill will allow an authorising officer of the Australian Federal Police or a Police Force of a State to access historical telecommunications data if it is relevant to locating a missing person. The amendments ensure that missing person information is only able to be used for the purpose of locating a missing person. The amendments also provide additional safeguards for the secondary disclosure of telecommunications data accessed specifically in relation to a missing person.

When the missing person information is obtained, it may only be disclosed to third parties to assist in locating the missing person. Importantly, missing person information may only be disclosed to the person who made the missing person report if the missing person is deceased or with the missing person's consent or to prevent a threat to the missing person's health, life or safety. These restrictions will ensure that the privacy of the missing person is respected and the information is only disclosed without the consent of the missing person if it is for their benefit. Agencies will also be required to report on the number of authorisations in relation to missing persons made by their agency.

The amendments in relation to a missing person will not impact on the operation of the existing access to telecommunications data provisions. Rather the amendment is a specific exception to the current regime and will be subject to stringent safeguards to maintain a person's privacy.

1.3.2 Victims of crime

A stored communication is defined in the TIA Act as a communication that is not passing over a telecommunications system, is held on a carrier's network and can only be accessed with the assistance of a carrier. Accessing a stored communication does not involve intercepting a communication as it occurs. Store communications includes information such as voicemail or short messaging service (SMS) messages.

Access to a person's stored communications requires a warrant to be issued by a judge or nominated Administrative Appeals Tribunal member. The issuing authority must consider a wide variety of factors, including how the privacy of the person would be impacted. Currently, warrants can be issued to access the stored communications of people 'involved in' a serious contravention. Due to the strictness of the privacy protections in the TIA Act the phrase 'involved in' has been interpreted as being limited to perpetrators. Access to the stored communications of a victim can provide valuable information in relation to victims of serious contraventions. Enforcement agencies can currently access stored communications under a search warrant where the victim can be notified and therefore have knowledge that their stored communications will be obtained in order to investigate the contravention. However the victim may not always be able to be notified (for example if they are missing, incapacitated or deceased).

To overcome this gap in policy, the Bill will allow enforcement agencies to access the stored communications of victims of crime if the victim cannot be notified that a law enforcement agency wishes to access their communications. The Bill will not change the ability of law enforcement agencies to access stored communications under a search warrant when the victim can be notified that those communications will be obtained. The Bill will not amend the requirement that stored communications can only be covertly accessed under a stored communications warrant from an issuing authority for offences that meet the appropriate offence threshold. Further, before issuing a stored communications warrant, the issuing authority will be required to be satisfied that the victim cannot consent, or that it is impractical for the victim to consent, to their stored communications being accessed. Agencies that obtain stored communications under these provisions will be required to report on the number of warrants obtained and be subject to oversight.

1.4 Industry operations

1.4.1 Notification of changes to telecommunications capability

The TIA Act currently places an obligation on carriers and nominated carriage service providers (C/NCSPs) to provide assistance to interception agencies. To facilitate this obligation, C/NCSPs are required to submit an annual interception capability plan (IC plan) to the Communication Access Co-ordinator (the CAC). The CAC is a statutory position created under the TIA Act. An officer of the Attorney-General's Department, currently the First Assistance Secretary of National Law and Security Division fills the role. The CAC is the primary point of liaison between interception agencies and industry and plays a major role in assisting members of industry to comply with their legislative obligations to provide reasonably necessary assistance to Australian law enforcement and national security agencies.

A C/NCSP is required to submit a revised IC plan to the CAC as soon as practicable following changes in the business plan that are likely to have a material adverse effect on their ability to comply with obligations for interception capability. This mechanism ensures agencies are aware of each C/NCSP's abilities to comply with their obligation over the 12 month period. Notification of a changed business plan is only required after a change is made.

The Bill requires C/NCSP to notify interception agencies, through the CAC of changes to telecommunications services, networks, systems or devices that would adversely affect the ability to conduct interception or to comply with relevant requirements in the *Telecommunications Act 1997* (Telecommunications Act) prior to their implementation. The Bill also provides a procedure for the CAC to engage in consultation with agencies and industry following notification.

The amendments are modelled on Division 4 of Part 15 of the Telecommunications Act which was repealed in 2007. When the IC plan regime was implemented in the TIA Act in 2007, it was thought that the corresponding notification obligations in the Telecommunications Act were redundant and were therefore repealed. However in practice, the IC plan does not facilitate notice sufficiently early in the development of a change to allow for effective consultation. Earlier notification will enable any changes that may adversely impact a C/NCSP to comply with their legal obligations to identified and worked through before implementation.

1.4.2 Notification of warrants

Carriers and carriage service providers (C/CSP) need to be formally notified of the existence of a warrant before they can offer assistance to law enforcement agencies. The TIA Act requires an agency to notify the Managing Director of a C/CSP of the existence of a warrant.

Currently the Managing Director of a C/CSP cannot nominate anyone else within the company to receive the notification, meaning a warrant cannot be executed if the Managing Director is not readily available. The Bill will allow a law enforcement agency to notify an 'authorised representative' of a C/CSP about the issue of and the revocation of telecommunications interception and stored communications warrants. An authorised representative will be defined as the Managing Director or the Secretary or an employee of the C/CSP who has been authorised in writing by the Managing Director. This amendment will apply to any warrant that has been issued before or after the Schedule commences, where a notification referred to in one of the amended provisions has not been made.

Allowing the delegation of warrant responsibilities will remove a significant regulatory and administrative burden on Managing Directors. Given the nature of the telecommunications industry, being able to delegate to an authorised delegate may also prevent sensitive warrant information from leaving Australia and investigations from being stymied by the unavailability of a C/CSP's Managing Director.