Australian Government

Attorney-General's Department

Supplementary Submission to the Senate Legal and Constitutional Affairs Committee

Intelligence Services Legislation Amendment Bill 2011

This is a supplementary submission to the Senate Legal and Constitutional Affairs Committee on the Intelligence Services Legislation Amendment Bill 2011 (the Bill). This submission focuses on the issues raised in the submissions to the Committee from the Castan Centre for Human Rights Law and Dr Dan Svantesson of Bond University. Further detail on the provisions in the Bill can be found in the Department's submission to the Committee. Our earlier submission also responded to the key concerns raised by the Law Council in its submission to the Committee.

Issues raised by the Castan Centre for Human Rights Law

In its submission to the Committee, the Castan Centre for Human Rights Law raised two areas of concern with the Bill. Firstly, the Castan Centre expressed concern about the potential of items 3 and 7 to increase the scope of ASIO's foreign intelligence collection powers. Secondly, the Castan Centre noted a potential constitutional complication that arises as a result of items 19 and 26.

Definition of foreign intelligence under the ASIO Act [Item 3]

Item 3 of the Bill will repeal the current definition of 'foreign intelligence' in section 4 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), and substitute a new definition. This new definition will align the definition of 'foreign intelligence' under the ASIO Act with the *Intelligence Services Act 2001* (IS Act) and *Telecommunications (Interception and Access) Act 1979* (TIA Act).

This will ensure that the collection of foreign intelligence under the ASIO Act encompasses the same range of intelligence about state and non-state sponsored threats as covered by the term 'foreign intelligence' in those other Acts. Similar amendments to the TIA Act were made in the *Anti-People Smuggling and Other Measures Act 2010*. This will enhance interoperability and intelligence sharing between agencies, as 'foreign intelligence' will have a consistent meaning among the Australian Intelligence Community (AIC) agencies, which will enable more efficient processes and arrangements for collecting and communicating foreign intelligence.

As ASIO's foreign intelligence collection function complements the foreign intelligence collection function of the other intelligence agencies, it is desirable that ASIO be able to collect intelligence about the same spectrum of threats as those agencies. With the current differences between the ASIO Act and the IS Act, there is some potential for gaps in

intelligence coverage as the ASIO Act definition of foreign intelligence is currently limited to intelligence about foreign powers.

- When the foreign intelligence function was initially conferred on ASIO, the key national security concern at the time was state sponsored threats. The definition of foreign intelligence in the ASIO Act reflected this, by defining foreign intelligence as 'intelligence relating to the capabilities, intentions or activities of a foreign power'.[1] Foreign power is defined as 'a foreign government; an entity that is directed or controlled by a foreign government or governments; or a foreign political organisation'.[2]
- When the IS Act was drafted, the concept of foreign intelligence reflected in the functions of those intelligence agencies was intelligence 'about the capabilities, intentions or activities of people or organisations outside Australia', in so far as this relates to 'Australia's national security, Australia's foreign relations or Australia's national economic well-being'.[3] This concept of foreign intelligence reflects that modern national security threats come from both state and non-state sponsored actors For example, terrorism, transnational crime, weapons proliferation and people smuggling are increasingly not sponsored by states, but rather by individuals or non-state sponsored organisations.

Foreign intelligence warrants under the ASIO Act [Item 7]

In addition to amending the definition of foreign intelligence to provide consistency, it is also necessary to amend the provisions relating to foreign intelligence collection warrants to align the collection of foreign intelligence under the ASIO Act and the IS Act. We note that the Castan Centre has raised concerns about the breadth of the amendment. Given that the objective is to ensure that ASIO's foreign intelligence function effectively complements the functions of the other foreign intelligence agencies, the relevant provision needs to reflect the same intelligence and the same purposes for which that intelligence may be obtained under the IS Act. If not aligned, there are some potential gaps in Australia's intelligence coverage.

ASIO's core function is to obtain and assess intelligence and advise government in relation to matters relevant to security, such as counter-terrorism and counter-espionage. The collection of foreign intelligence outside Australia is, and will continue to be, the responsibility of Australia's foreign intelligence agencies, under the IS Act.

ASIO's existing function to obtain foreign intelligence is limited to within Australia, in order to complement the role of the foreign intelligence agencies. This limitation is not being changed by the proposed amendments. This function is only exercised at the request of Australian foreign intelligence agencies, under warrant signed by the Attorney-General, and on advice from the Minister for Defence or Minister for Foreign Affairs. The Attorney-General will be required (under the proposed amendment) to be satisfied that collecting particular intelligence is in the interests of Australia's national security, Australia's foreign

[1] *Australian Security Intelligence Organisation Act 1979*, section 4.

[2] Ibid.

[3] *See, Intelligence Services Act 2001,* section 11.

relations or Australia's national economic well-being. These are serious matters of significant national interest.

It is not expected that this amendment will result in significantly more foreign intelligence collection warrants being issued under the ASIO Act. ASIO's foreign intelligence function, as with all its activities, is subject to rigorous oversight and accountability, including by the Inspector-General of Intelligence and Security (IGIS), whose role is to review the legality *and propriety* of ASIO's activities.

As noted above, the IS Act limits the concept of foreign intelligence by requiring that the agencies' functions 'are only to be performed in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being'.[4] The current provisions in the ASIO Act enable the Attorney-General to issue a warrant for ASIO to collect foreign intelligence if satisfied, on the basis of advice from the relevant Minister, that the intelligence is important in relation to the defence of the Commonwealth or the conduct of the Commonwealth's international affairs.[5] The proposed amendment will provide consistency with the IS Act by requiring the Attorney-General to be satisfied, on the basis of advice from the Defence Minister or Foreign Affairs Minister, that the collection of intelligence is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being. The effect of these amendments is that ASIO's foreign intelligence collection function will provide a consistent and complementary role to the other agencies where it is necessary to collect foreign intelligence within Australia.

The amendments are not connected with any particular matter, and are a continuation of an amendment process initiated long before the Wikileaks matter.

Immunity provisions in the IS Act and Criminal Code [Items 19 and 26]

The Castan Centre noted a potential constitutional complication may arise as a result of items 19 and 26. The Bill will amend the IS Act to clarify that the immunity provision in section 14 is intended to have effect unless another law of the Commonwealth, a State or Territory expressly overrides it. This provision provides immunity from civil and criminal activities for a limited range of circumstances directly related to the proper performance by the agencies of their functions. A similar amendment will also be made to the immunity provision for the computer offences in Part 10.7 of the Criminal Code to clarify that the provision is intended to have effect unless another law of the Commonwealth, a State or Territory expressly overrides it.

As currently drafted, the provisions are vulnerable to a law that is later-in-time inadvertently overriding them. This could occur particularly where an Australian law has extra-territorial effect. The Bill will amend the IS Act and the Criminal Code to clarify that the immunity provisions are intended to have effect unless another law of the Commonwealth, a State or Territory expressly overrides these provisions.

[4] Ibid.

[5] *Australian Security Intelligence Organisation Act 1979*, paragraphs 27A(1)(b) and 27B(b).

The Department considers the Castan Centre's view that there is a potential constitutional complication arising out of items 19 and 26 to be overstated. The normal rules of statutory construction provide that an earlier statutory provision is not repealed by a later provision unless an intention to that effect is implied (for example, the provisions are not capable of operating consistently). There is a general presumption that the legislature intends that both provisions should operate and that, to the extent they would otherwise overlap, one should be read as subject to the other.[6]

The proposed amendments would make it clear that the provisions are intended to prevail in the absence of an express contrary provision. This makes the legislature's intention clear as to the intended operation of the law. In the absence of clear indication by a later legislature that it intends to displace these express provisions and impliedly 'repeal' them, the proposed amendments to the immunity provisions may operate to affect the question of precedence between overlapping provisions in relevant cases.

The proposed amendments will not prevent other laws from limiting the immunity in these provisions as Parliament may choose to override these immunities in appropriate circumstances. The immunity provisions are not necessarily something that legislators would actively turn their mind to, and the risk of inadvertently overriding these provisions could therefore arise. However, the amendments will ensure that there would need to be a conscious decision to do so and it would need to be made express on the face of the legislation. This would ensure that any such limitation cannot be done inadvertently.

Issues raised by Dr Dan Svantesson

ASIO computer access warrants [Item 4]

In his submission to the Committee, Dr Dan Svantesson of Bond University noted that the wording in paragraph 25A(4)(a) of the ASIO Act remains focused on data present on a particular computer, and this may mean that the warrant would not authorise the collection of data that is associated with the target computer through a cloud computing arrangement.

The Bill will amend paragraph 25A(4)(a) of the ASIO Act to replace 'stored in the target computer' with 'held in the target computer at any time while the warrant is in force'. This amendment is not intended to change the law, but rather to clarify the intent of the provision and ensure consistent language is used throughout the provision.

The scope of this amendment is to clarify that the intention was to authorise access to data held in the target computer at any time while the warrant is in force. This makes clear that the provision is intended to authorise access to data that is held in the target computer during the life of the warrant, and is not limited to data held at a particular point in time (such as when the warrant is first executed).

[6] *Saraswati v R* (1991) 100 ALR 193; per Gaudron J at 204.

Currently, the computer access warrant provision uses different language in different subsections in relation to the same concept. Subsection 25A(2) refers to 'data *held* in a particular target computer', whereas paragraph 25A(4)(a) refers to 'data... *stored* in the target computer'. The proposed amendments will provide consistent language in the provision.

The term data 'held' in the target computer is preferred as the more technologically neutral term. It would clearly encompass data that is stored on a more permanent basis, such as in a hard drive, as well as data that may be held in the computer on a temporary basis or from time to time, as is the intention of the provision. The amendment further clarifies this intent by providing that the Attorney-General may issue a computer access warrant 'for the purpose of obtaining access to data that is relevant to the security matters and is held in the target computer *at any time while the warrant is in force*'.

Section 22 of the ASIO Act provides a number of definitions for the purpose of interpreting the computer access warrant provisions under section 25A of the ASIO Act. These definitions are technologically neutral and provide authoritative and useful definitions for ASIO in the exercise of its powers under section 25A. The definitions are wide enough to include various aspects of a computer and types of data. Under section 22 of the ASIO Act, computer means 'a computer, a computer system or part of a computer system' while the definition of data 'includes information, a computer program or part of a computer program'.

Finally, the Department would like to note that ongoing consideration and active review is undertaken to ensure that Australia's national security agencies continue to have the necessary tools to undertake their important functions.