Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014

SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

Organisation:

Muslim Legal Network(NSW)

Birchgrove Legal

Name:

Rabea Khan, Mahmud Hawila, Moustafa Kheir, Hisham Karnib, Khodr Ghantous, Nandan Subramanian, Sarah Khan and Yusra Metwally.

With special thanks to Mr Peter Lange of Counsel

Other organisations in support of this submission:

Muslim Legal Network (VIC)

Muslim Legal Network (WA)

WHO WE ARE

The **Muslim Legal Network (NSW)** is an Australian-based legal practitioner and law student association. It is a gateway for Australian Muslim law students and legal practitioners to both network with one another and engage with the wider legal community.

Birchgrove Legal is a boutique Sydney based law firm. Our lawyers practice in administrative law and criminal law. Birchgrove Legal prides itself on protecting rights and committing its pro- bono efforts for community value adding. Our firm advocates social responsibility and aims to do so using all tools including engaging in both the political and commercial worlds.

Contact:

Muslim Legal Network (NSW): 0412 944 173, muslimlegalnetworknsw@gmail.com

GENERAL REMARKS ON THE INQUIRY AND THE DISCUSSION PAPER

The Muslim Legal Network (NSW) and Birchgrove Legal welcome the opportunity to provide the following submission to the PJCIS Inquiry into the National Security Legislation Amendment Bill (2014) (the Inquiry).

TIME RESTRAINTS OF THE INQUIRY

On 16 July 2014 the Attorney-General, Senator The Hon George Brandis, asked the Committee to inquire into and report on the National Security Legislation Amendment Bill (No. 1) 2014 (the Bill). Submissions for this inquiry were due on 6 August 2014, public hearings to commence on 11 August 2014 and PCJIS Report to be presented to Parliament on 7 September 2014.

The limited time provided for submissions has been cause for restrictions in our submissions. A lengthier time frame would have provided us with a greater opportunity to engage in community consultation. Given the short time frame, the necessary community consultation was not feasible. Furthermore, many of the changes proposed in the Bill that are subject to this inquiry are technical in nature and require a considered and detailed legal analysis. The time restraints were a limitation to our submission in that regard also.

We are extremely concerned at the speed in which the proposed Bill is travelling through Parliament. The Bill proposes a large number of significant changes to national security legislation, which will severely impact on the civil liberties of ordinary Australian citizens, most notably, their privacy and right to a fair trial

The proposed amendments, with their broad nature and limited safeguards for civil liberties will undoubtedly work to invite fears about the culture of unaccountability within intelligence and law

enforcement agencies.

Consequently, we note that such a vital inquiry should be conducted within a reasonable time timeframe to allow for consideration and consultation by and with the public.

We would also like to highlight that various Muslim community leaders and organisations Australia wide have presented a unified response and have vocally expressed their concerns in recent days about the proposed laws, and the concerning degree of lack of community consultation. The recent press conference with the Prime Minister calling for 'Team Australia' to be behind these proposed laws only serves to place the spotlight on the Muslim community, once again questioning the place of Muslims in Australia. Given the rise in Islamophobia and discrimination, we would respectfully submit that such language is unhelpful and has the danger of creating a divisive society to further marginalise the Muslim community. The objections and concerns of Muslim community leaders and organisations are expressed as concerned Australian citizens, not as a sub group of society.

In consideration of the above, we reserve the right to provide supplementary submissions in areas that are not sufficiently addressed within this submission.

SCOPE OF THIS INQUIRY

It is unfortunate that the scope of this inquiry is limited to Chapter 4 of the 2013 Report of the Inquiry into Potential Reforms of Australia's National Security Legislation. There have been a large number of proposed laws announced before and during the period of this inquiry that are outside of the terms of reference for this inquiry. These changes are significant and involve the investigation and prosecution of Australian citizens who may choose to take part in foreign conflicts. We are concerned that no details or draft legislation have been provided in relation to

these proposed laws and that they have not been made available for public consultation.

As those proposals and changes to laws concerning data retention are outside the scope of this inquiry, we are not able to comment on them in this submission.

TABLE OF CONTENTS

1. Changes to ASIO employment provisions

a) ASIO secondment arrangements……6

b) Identifying ASIO officers……..8

2. **Changes to ASIO warrant provisions**

a) Definition of ‘computer’……9

b) Creation of a named person warrant……11

c) Authorisation lists for warrants……...12

d) Use of force in execution of warrants……13

e) Evidentiary Certificates……15

3. Activities and functions of Intelligence Services Act 2001 agencies……17

4. Creation of Authorised Intelligence Operations Scheme……....19

1. CHANGES TO ASIO ACT EMPLOYEE PROVISIONS

a) ASIO Secondment arrangements

The Bill proposes to insert sections 86, 87 and 88 into the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). These new sections serve to align the ASIO Act employment provisions with that of the *Public Service Act 1999* in order to access specialist skills and as a part of arrangements whereby ASIO works closely with other agencies. These new sections provide additional scope for further secondment arrangements for ASIO officers into other agencies and for officers from other agencies into ASIO and attempt to address recommendation 26 in Chapter 4 of the 2013 Report of the Inquiry into Potential Reforms of Australia's National Security Legislation (the Report).

We are concerned that the proposed provisions create a framework with the potential to allow for the circumvention of existing statutory limitations. The Inspector-General of Intelligence and Security submitted that "*it would not be proper for an ASIS staff member to be 'seconded' to ASIO for a day or two to enable them to perform an activity which it would otherwise not be permitted to undertake. My understanding is that this is not a practice the agencies intend to adopt".*[1]

It is respectfully submitted that additional safeguards should be introduced into the aforementioned sections in order to ensure their proper use. No such safeguards are specified within the Bill; therefore we cannot comment further at this stage.

It is also submitted that these proposed amendments are likely to blur the line between agencies who are otherwise distinct and separate. Legal complexities arise from these arrangements, especially in the case of overseas operations. We therefore, agree with the view

[1] Inspector-General of Intelligence and Security, *Submission No. 185,* p. 16.

of the Inspector-General of Intelligence and Security that it is important to ensure that 'changes are applied in such a way that is clear to individual officers which agency they are undertaking an activity for and that 'secondments' are a true change in working arrangements for a period.'[2]

It is in the interests of the Government to ensure that new powers awarded by these provisions are also met with the necessary checks and balances, which encourage their transparent and proper use.

b) Identifying ASIO officers

The Bill seeks to insert a new subparagraph 18(3)(b)(ia) into the *Australian Intelligence Organisation Act 1979*.

We object to the existence of Section 92 of the ASIO Act in its current and proposed formulation. We respectfully submit the public disclosure of an ASIO officer's identity is in the public interest in some circumstances. Section 92 in its current and proposed form prohibits the publication of the names of ASIO officers.

The Report did not find it to be in the public interest to allow the publication of the identity of ASIO officers. Whilst we agree that non-publication is generally in the interests of the safety of ASIO employees and ASIO's inherent secrecy, we do however, respectfully submit that this should not be a blanket provision. We submit that it will be in the public interest that the identity of ASIO officers be published when involved in criminal acts.

[2] Ibid

3. CHANGES TO ASIO WARRANT PROVISIONS

a) Definition of 'computer'

2.1 The Bill proposes that the ASIO Act is amended so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network. The current legislative framework provides that if an individual has more than one computer, which is not part of the same computer system, or data is stored on a computer network, it may be necessary for the Attorney General to issue more than one warrant. Computer access warrants under section 25A of the current ASIO Act are limited to obtaining data stored on 'a computer', which limits its scope to a particular computer in question rather than any number of computers accessed by an individual. This is addressed in Recommendation 20 of the Report.

The explanatory memoranda states that the Bill will modernise the definition of 'computer' to enable it to include a computer network to cover situations where individuals are associated with multiple computers or networks, thus allowing ASIO to obtain intelligence from a number of computers or networks under a single computer access warrant. The Bill expands what can be covered by the target computer of a computer access warrant to include any combination of one or more computers, computers on particular premises and computers associated with a specified person.

2.2. We respectfully submit that the scope of 'computer network', as proposed by the amendment is far too broad and could prejudicially impact an unsuspecting third class of persons in its application, such as an entire workplace. Additionally, broadening the scope of 'computer network' would be operationally inefficient and thus could potentially constitute a wasteful use of valuable public resources, in additions to the clear invasive breach of privacy.

Given the lack of explicit legislative provision stating the need to establish a connection between the use of an individual's computer and the use of computers across the computer network, a warrant for an entire 'computer network' is far too broad. We also share the concerns expressed in the 2013 inquiry by Mr Ian Quick and the Gilbert + Tobin Centre of Public Law.

The explanatory memoranda also states that the Bill will amend section 25A so that ASIO will be able to use a third party computer or communication in transit (and add, copy, delete or alter data in the third party computer or communication in transit) for the purpose of obtaining access to data relevant to the security matter and that held on the target computer. ASIO may only do so where it is 'reasonable in all the circumstances', having regard to other methods of obtaining access to the data which are likely to be as effective.

It is submitted that the proposed amendment severely infringes upon the rights of third parties who may not be related to the investigation or an alleged commission of a crime in question. We respectfully submit that rights of third parties to privacy should take precedence over operational considerations/efficacy, regardless of how minor the interference may be.

Additionally, a significant issue arises in foreseeable situations where a particular computer network is monitored and other unrelated evidence is uncovered in relation to a person who is not subject to an investigation. The admissibility of such evidence to be disseminated and referred to other law enforcement agencies will be in question. This may also create opportunities for the exploitation of third party data and personal information for various purposes not defined in the application for a warrant that do not have a legitimate forensic purpose , leading to a potential 'fishing expedition'.

Therefore, although the Bill implements Recommendation 20 of the Report, we respectfully submit that it does not adequately balance national security and safeguards that protect the rights of ordinary Australian citizens.

b) Creation of a Named Person Warrant

The Bill proposes to amend the ASIO Act to enable the issuing of an identified person warrant, which would enable ASIO to seek one warrant specifying a number of powers against the identified person. Under the current legislative framework, the ASIO Act requires the agency to submit an application requesting each individual power to be granted, which has been perceived to create administrative and operational inefficiencies. These issues are related to Recommendation to 29 of the Report.

The explanatory memoranda states that in order for this identified person warrant to be issued, the Minister 'must be satisfied that the person is engaged in, or is reasonably suspected by the Director-General of being engaged in, or likely to engage in activities prejudicial to security and the issuing of the warrant in relation to the person, will, or is likely to, substantially assist the collection of intelligence relevant to security.'

It is respectfully submitted that the considerations of administrative and operational efficiency should not be allowed to outweigh concerns of the individual's right to privacy. Condensing multiple powers into a single warrant sidesteps the concern that the greater the incursion into privacy, the greater threshold there ought to be. It is important to acknowledge the fact that under the current legislative framework, the requirement for various warrants recognises the distinctions between different warrants and incursions into a person's privacy. For example, the installation of surveillance cameras in a private dwelling would be a far greater incursion into a person's privacy than a tracking device on their vehicle, and should be considered separately for this reason.

Furthermore, allowing the identified person warrant to be in operation for a maximum period of six months, as is stated in the explanatory memoranda, is far too long given its wide potential scope. While we note that the Minister may revoke the warrant or place restrictions upon it while

it remains in force, we believe that this discretion would be more appropriately vested in the judiciary rather than be left to a matter of good administrative practice.. It is noted that urgent warrants can be applied for and granted by the Judiciary when needed. Any requirement to reapply for a warrant before a member of the judiciary need not be regarded as an impediment; rather, it would safeguard the provision.

Therefore, although the Bill implements Recommendation 29 of the Report, we respectfully submit that this amendment also it does not adequately balance national security and safeguards that protect the rights of ordinary Australian citizens.

c) Authorisation Lists for Warrants

Currently, section 24 of the ASIO Act provides that the Director-General, or senior officer authorised in writing by the Director General, may approve certain officers and employees to execute warrants issued under Division 2 of Part III of the ASIO Act. The Bill proposes to repeal this section and instead allows for the Director-General or senior officer to approve a person or class of persons as being able to execute the authority of a warrant. This amendment responds to Recommendation 32 of the Report.

It is respectfully submitted that while this amendment may increase operational efficiency, it is necessary to ensure that this class of persons is of the appropriate ranking and are in possession of the appropriate qualifications and training to be dealing with the execution of these warrants. It is also important to ensure that external parties used to execute the warrant, such as telephone carriers, are aware of who constitutes this class of persons and that all their dealings are only conducted with this class of persons.

d) Use of force in execution of warrants

The Bill proposes to clarify the use of reasonable and necessary force during the execution of warrants in Sections 25(5A)(a), 25(7)(a) and 27A(2)(a) of the *Australian Security Intelligence Organisation Act 1979.*

Sections 25(5A)(a), 25(7)(a) and 27A(2)(a) of the Act relate to computer warrants, search warrants and warrants in relation to foreign intelligence and authorise the use of any force that is necessary and reasonable to do things specified in the warrant. The Bill proposes to insert the words “against persons and things” after the words “any force” in the abovementioned sections in order to clarify the meaning and application of “force”.

The explanatory memoranda states that the force may be used at any time of the warrant, providing the example that it may be necessary to use force to obtain access to an object on premises under investigation, such as a door or a cabinet lock or to use force to install or remove a surveillance device.

It is respectfully submitted that such an amendment is unnecessary and superfluous, given the fact that the abovementioned sections currently already permit the use of *any* force that is necessary and reasonable to do the things specified in the warrant. Under the current legislative framework, the inclusion of the word ‘any’ is broad and already covers any actions performed at any time during the execution of a warrant and obtaining access to a thing on the premises or installing or removing a surveillance device so long as the reasonable and necessary force in question is used to carry out what is specified in the warrant.

The explanatory memoranda further states that the use of force would extend to using reasonable and necessary force against a person in situations where a person tries to obstruct the execution of a search warrant. This has not been specified in the Bill. It is respectfully submitted, for the purposes of clarity, that a subsection be provided in Sections 25(5A)(a),

25(7)(a) and 27A(2)(a) stating this expressly. If this is expressly stated, the insertion of the words “against persons and things” becomes even more unnecessary. This would also act as a safeguard for members of the community who are subject to such warrants by limiting any force used against them to situations where there is obstruction of the execution of a warrant.

We further submit that the wording of Section 34V(2) and (3) of the *Australian Security Intelligence Organisation Act 1979* be adopted for situations where reasonable and necessary force be used towards a person, that is:

> (2)‘in relation to a person, use more force, or subject the person to greater indignity, than is necessary and reasonable to do the act;’ and
> Without limiting the operation of subsection (2), an officer must not, in the course of an act described in subsection (1) in relation to a person:
>
> > (a) do anything that is likely to cause the death of, or grievous bodily harm to, the person unless the officer believes on reasonable grounds that doing that thing is necessary to protect life or to prevent serious injury to another person (including the officer); or
> >
> > (b) if the person is attempting to flee during a warrant – do such a thing unless:
> >
> > > (i) the officer believes on reasonable grounds that doing that thing is necessary to protect life or to prevent serious injury to another person (including the officer); and
> > >
> > > (ii) the person has, if practicable, been called on to surrender and the officer believes on reasonable grounds that the person cannot restrained in any other manner.

It is submitted that this would more effectively ensure the balance of national security and safeguards. We also note that this change was not discussed or recommended in the Report.

e) Evidentiary Certificates

The Bill proposes to insert Section 34AA to the *Australian Security Intelligence Organisation Act 1979.* This new section is proposed to allow the creation and tender of evidentiary certificates in relation to foreign intelligence warrants relating to computer access and identified person warrants relating to computer access and surveillance devices. It provides a list (which is not limited) to matters an evidentiary certificate can cover relating to how a warrant was executed and by whom. These certificates are prima facie evidence of matters stated in the certificate.

We oppose the inclusion of this section as proposed.

A fundamental part our criminal justice system is the presumption of innocence. Pursuant to Article 14(2) of the *International Covenant of Civil and Political Rights*, the prosecution bears the onus of proof and holds an obligation to prove all elements of an offence beyond reasonable doubt. There are only a small number of offences where the onus of proof is on the accused, which is usually subject to the lower standard of on the balance of probabilities, such as deemed supply of prohibited drug offences.

Although, these certificates are persuasive rather than conclusive, they nevertheless shift the burden of proof on to the accused as they are considered prima facie evidence. We find this to be a direct contravention of the right to a fair trial, the presumption of innocence and the right to silence. The explanatory memoranda states that the certificate ‘requires the defendant to disprove the matters certified in the evidentiary certificate if they seek to challenge them’.

We appreciate that evidentiary certificates are common place in the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* and we agree that it may be appropriate with warrants under Sections 25A and 26 to allow evidentiary certificates.

However, we do not agree with the allowance of evidentiary certificates under Section 29. Section 29 includes Section 27 warrants, which are much more intrusive in nature than the others. We respectfully submit that evidentiary certificates should not be extended to Section 29.

We understand the need to protect the technological capabilities of ASIO, however respectfully submit that current procedures under Public Interest Immunity are sufficient to address this concern for warrants under Section 29.

ACTIVITIES OF FUNCTIONS OF INTELLIGENCE SERVICES ACT 2001 AGENCIES

Recommendation 27

The Committee recommended that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.

Paragraph 6B(e)(ii) and new paragraph 6B(e)(iia), Schedule 5 of the Bill attempts to further clarify the functions of the Defence Imagery and Geospatial Organisation (DIGO). Current powers under Section 6B of the IS Act details that the functions of DIGO are concerned with obtaining geospatial and imagery intelligence about: 'the capabilities, intentions or activities of people or organisations outside of Australia'; 'for the purposes of meeting the operational, targeting, training and exercise requirements of the Defence Force'; and 'for the purposes of supporting Commonwealth authorities and State authorities in carrying out National Security functions'. In particular, the current Section 6(e) is characterised with vague terms, which allows the DIGO to provide the obtained information to Commonwealth and State authorities and bodies that have been approved by the Defence Minister.

Proposed amendments aim to dispose any doubt that DIGO is able to provide these authorities with both non-intelligence and intelligence imagery and geospatial products using express terms.

The amendments will enable DIGO to provide assistance to Commonwealth and State authorities and bodies approved by the Minister in relation to the provision of technical assistance in the production and use of all imagery and geospatial products and assistance in relation to technologies as well as products.

In targeting certain individuals who pose a threat, the amendments will allow DIGO to work with other agencies, like ASIS and DSD, to obtain intelligence and cooperate with ASIO in the

execution of its functions. The functions of the DIGO are very strong intelligence powers and as such, amendments to any provision have a large effect on their operations. There is a concern that the absence of provisions that hold the Organisation and its limbs accountable, will engender a situation where these powers are abused.

The Recommendations claim that the amendments, being only minor clarifications, would not affect the powers and safeguards already in place. These include Ministerial authorisations and Privacy Rules in relation to disclosure of intelligence about an Australian person made under section 15 of the IS Act.

Section 11 provides for the limits on DIGO's powers whilst Section 12 outlines the limits on its activities. Both sections will continue to apply with the proposed amendments and strongly advocate that the functions of the organisation should only be performed in the interests of Australia's national security, Australia's foreign relations or national economic well-being and only to the extent that these matters are affected by the activities of people or organisations outside of Australia.

The clarification of the powers and functions of DIGO is significant. However, the clarification is not *just* a clarification. The proposed amendment will expressly outline that DIGO is free to work with and assist Commonwealth, State authorities and other bodies approved by the Defence Minister in the interests of Australia's national security.

Such a proposed legislative framework is indicative that intelligence agencies such as ASIS, DSD and DIGO will be involved in a process of information sharing of collected data. We are concerned with the lack of a complementing proposed clause to details of any limitations as to the extent by which information sharing can occur, the type of data that can be shared and the specified time period in which this can occur. Consequently, information that has been collected since the organisation's establishment may be freely shared amongst different government

departments. This also extends to data that is currently being amassed and may be distributed to other departments well into the future.

Essentially, the intelligence that is shared will be predominantly related to the tracking of individual activity. The mass collection and distribution of such information amongst government agencies has the potential to destroy the fabric of an individual's right to privacy. Such undertakings are not dissimilar to the operations and mass surveillance of the National Security Agency (NSA) in the United States. The extent to which NSA spied on persons inside and outside their sovereign invited widespread criticism. The proposed methodology of sharing surveillance information across Australian agencies may result in a highly risky emulation of surveillance methodologies in the USA,

4. Creation of an Authorised Intelligence Operations Scheme

This Bill seeks to amend Part III of the *Australian Intelligence Organisation Act 1979* by inserting Division 4 to create an authorised intelligence operations scheme. This scheme would provide ASIO officers and its human sources with protection from criminal and civil liability for certain conduct within the course of authorised intelligence operations.

We reject the analogy made linking this proposed scheme and that of the existing Australian Federal Police (AFP)'s controlled operations. We respectfully submit ASIO does not require such legal immunities.

With respect to the submissions made by Dr Patrick Emerton of the Castan Centre for Human Rights Law at Monash University, we also submit ASIO is in a *"very different constitutional position, a very different administrative position and a very different policy position"* to the AFP.[5]

Furthermore, AFP activities are subject to a range of existing internal and independent accountability frameworks. This level of accountability oversight does not exist for ASIO operations. Although the Explanatory Memoranda suggests particular restrictions, reporting and accountability mechanisms, there is insufficient information to satisfy these deep concerns.

We respectfully submit that ASIO, unlike the AFP, does not require immunity from criminal and civil proceedings. The allowance for such immunity, albeit limited to the regime proposed, would reinforce the unaccountability of ASIO in its *"essentially secret"*operations[6].

It is our submission that this proposed regime does not protect the confidential nature of ASIO's undercover operations. We support the submissions made by the Gilbert + Tobin Centre of Public Law in this regard, with reference to the 'highly unlikely' chance ASIO or ASIO officers would be prosecuted for undercover activities due to the Commonwealth Director of Public Prosecution (CDPP)'s discretionary power on whether or not to prosecute.[7]

We also submit that this discretionary power held by the relevant Director of Public Prosecutions sufficiently protects ASIO employees and affiliates in the course of their work from the theoretical possibility their activities could potentially result in criminal or civil liability. These discretionary powers serve as an external mechanism, which determines whether or not to pursue a prosecution on a case-by-case basis, and should be reinforced as such.

[5] Dr Patrick Emerton, Castan Centre for Human Rights Law, *Transcript*, Melbourne, 5 September 2012, p. 21; see also NSW Council for Civil Liberties, *Submission No. 175*, p. 13; Law Council of Australia, *Submission No. 96,* p. 58.
[6] Ibid.
[7] Gilbert + Tobin Centre of Public Law, *Submission No. 36*, p. 16.

It is also submitted, in the event that the Director of Public Prosecutions chooses to prosecute, strong protections at law exist to mitigate the risk of disclosing sensitive and confidential information, including closed court proceedings and Public Interest Immunity.

Although, the Committee at Recommendation 38 recommended that such a change be made, we respectfully submit that this change will be without appropriate safeguards and foster a culture within ASIO of unaccountability.