Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014

Pirate Party Australia

Arik Baratz
David Crafti
Andrew Downing
Mozart Olbrycht-Palmer
enquiries@pirateparty.org.au

6 August 2014

Contents

Introduction

Pirate Party Australia thanks the Parliamentary Joint Committee on Intelligence and Security for the opportunity to submit on such an important issue as reforms to national security legislation.

The Pirate Party's submission has focused on several areas of the National Security Legislation Amendment Bill (No 1) 2014 as they relate to civil liberties and transparency, especially the proposed expanded definition of 'computer', the introduction of an evidentiary certificate system, and the cumulative effects of particular amendments. The Pirate Party encourages the Committee to recommend against enacting the proposed amendments.

About Pirate Party Australia

Pirate Party Australia is a political party based around the core tenets of freedom of information and culture, civil and digital liberties, privacy and anonymity, and government transparency. It formed in 2008, and is part of an international movement that began in Sweden in 2006. Pirate Parties have been elected to all levels of government worldwide. The Pirate Party has been a registered political party under the *Commonwealth Electoral Act* since January 2013.

1 General remarks

The scope of the National Security Legislation Amendment Bill (No 1) 2014 ('the Bill') is wide and includes substantial administrative amendments alongside significant changes to intelligence powers and the introduction of new offences. The Parliamentary Joint Committee on Intelligence and Security ('the Committee') should recommend that these provisions be reintroduced as two (or more) separate bills if the Government and the Committee believe, after this inquiry is completed, that they should be pursued.

It is inappropriate to bury (unintentionally or otherwise) provisions that, for example, allow the Australian Security Intelligence Organisation ('ASIO') to 'add, copy, delete or alter' data on third party computers be-

tween provisions that amend the structure of ASIO.[1] Provisions altering the structure of ASIO should be separated from provisions conferring or altering ASIO powers and which amend or introduce new offences. Amendments to the internal structure and operations of ASIO are, while often necessary, comparatively meaningless to the public. Provisions that alter the powers of ASIO, change the level of oversight or create new or modify existing offences are of much greater public concern when issues of privacy and transparency may or will be negatively affected.

In an open letter to the Secretary of the Committee dated 29 July 2014, the Pirate Party requested an extension of two weeks from 1 August 2014 for submissions on the Bill.[2] This letter is included as Appendix A. The primary grounds for requesting the extension were the sheer length of the materials (124 pages for the Bill, 167 pages for its explanatory memorandum) and the seriousness of the amendments. The Pirate Party was informed that an extension had been granted (independently of the request) until 6 August. With respect to the Secretary and the Committee, this is still an insufficient amount of time to analyse and submit on the practical and theoretical effects of the proposed amendments, the enormity of which cannot be denied.

2 Restrictions on political communication

The definition of 'ASIO affiliate' and its inclusion in the replacement subsection 18(2) of the *Australian Security Intelligence Agency Act 1979* ('ASIO Act') substantially increases the pool of individuals to whom subsection 18(2) applies. The current subsection 18(2) applies where

> a person makes a communication of any information or matter that has come to the knowledge or into the possession of the person by reason of his or her being, or having been, an officer or employee of the Organisation or his or her having entered into any contract, agreement or arrangement with the Organisation, being information or matter that was acquired or prepared by or on behalf of the Organisation in connection with its functions or relates to the performance

[1] See eg National Security Legislation Amendment Bill (No. 1) 2014 (Cth) sch 2 item 41.

[2] Letter from Pirate Party Australia to the Secretary of the Parliamentary Joint Committee on Intelligence and Security, 29 July 2014 <http://pirateparty.org.au/2014/07/29/open-letter-to-the-pjcis/>.

by the Organisation of its functions[.]

The penalty for doing so is two years imprisonment, unless an exemptions applies.

The new subsection 18(2) would expand this through two proposed amendments: the first by schedule 1 items 1 and 6, and the second by schedule 6 item 2 of the Bill.

The proposed definition of 'ASIO affiliate' (sch 1 item 1) would expand subsection 18(2) to include persons 'performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement.' This is a significant expansion of the number of individuals section 18(2) applies to, and does not provide any metric by which to judge the seriousness of the communication or the public interest benefit in having certain information communicated. This would seem now to cover not just contractors, but employees of a contracting business and subcontractors they might engage.

The penalty for breaching section 18(2) is also significantly increased, from two years to ten years imprisonment (sch 6 item 1). This poses concerns given there does not appear to be any discretion or leeway provided to adjust the penalty to take into account the seriousness and intent of the breach.

Although it is not suggested that sensitive and current operational matters should be disclosed without good reason, there are certain instances in which the public interest justifies disclosure so that the public can make informed decisions about the actions of government and law enforcement and intelligence agencies. If everyone was restricted from talking about national security information it would almost certainly violate the freedom of political communication established by the High Court in, and developed since, 1992.[3]

ASIO already enjoys exemption from the *Freedom of Information Act 1982*,[4] making the organisation, in accordance with its nature, especially opaque.

However, broadening exemptions to transparency to include a larger group of people ought to be balanced by a publc interest test whereby the decision of an employee or affiliate to disclose certain information can be defended. Without such a public interest test, the legislation

[3] *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1.
[4] *Freedom of Information Act 1982* (Cth) s 7.

may fall foul of the freedom of political communication as the public already has limited knowledge of ASIO activities and is for the most part unable to make informed opinions as to the appropriateness of ASIO's operations.

Although the Attorney-General has, in Parliament, called former United States National Security Agency contractor Edward Snowden a 'traitor … who, through his criminal dishonesty and his treachery to his country, has put lives, including Australian lives, at risk',[5] those claims, which have also been made by representatives of governments and intelligence agencies in the US, UK and Australia, are not verified by actual evidence. While there is no evidence to support claims that Mr Snowden's release of information on operations of the National Security Agency and its international counterparts has caused such enormous public threat, debate by the general public, the media, and in the political system continues.

It is not suggested that extreme disclosures such as those made by Mr Snowden should be permitted. Nevertheless it is arguable that his actions are a symptom resulting from the lack of public disclosure mechanisms. The inability for the public to debate broad principles due to a lack of knowledge of the powers and actions government agencies including ASIO will naturally result in major, sensitive disclosures where individuals believe the public needs to be informed, or where the public is significantly uninformed.

The Committee should recommend against the Bill on the grounds that it provides insufficient protection of the public interest.

3 The definition of 'computer' and increased access

The expanded definition of 'computer' proposed under schedule 2 item 4 of the Bill is entirely inadequate and inappropriate, and demonstrates a lack of understanding of the technology being addressed.

The definition proposed is as follows:

> ***computer*** means all or part of:

[5] Commonwealth, Parliamentary Debates, Senate, 11 February 2014, page 29, (George Brandis, Attorney-General.

(a) one or more computers; or

(b) one or more computer systems; or

(c) one or more computer networks; or

(d) any combination of the above.

This is substantially broader than the current definition where 'computer means a computer, a computer system or part of a computer system'[6] but is no less, and is perhaps in fact more, ambiguous.

It is unclear what a 'computer' would, under the proposed or current definition, include. All of the following are, if the technical reality is accepted, considered a computer:

- Personal computers (desktops and laptops).
- Tablet computers.
- Mobile phones and smartphones.
- Servers.
- Google Glasses and similar devices.
- Self-service checkout machines.
- Automatic teller machine (ATMs).
- Digital televisions.
- DVD players.
- Certain network components
- Electronic control units in vehicles.
- Digital cameras.
- Satellite navigation systems.

The *Oxford Dictionary of English* provides a definition of 'computer':

> an electronic device which is capable of receiving information (data) in a particular form and of performing a sequence of operations in accordance with a predetermined but variable set of procedural instructions (program) to produce a result in the form of information or signals.[7]

This is a broad definition and certainly includes those examples provided.

[6] *Australian Security Intelligence Organisation Act 1979* (Cth) s 22.

[7] Angus Stevenson (ed), *Oxford Dictionary of English* (Oxford University Press, 3rd ed, 2010).

Jonathan Clough notes in *Principles of Cybercrime* that a definition of 'computer' in law is elusive and the Australian approach has been to to avoid defining the term in legislation due to a number of factors including the constant and rapid development of technology.[8] Clough adds, however, that 'increasing computerisation of many household appliance and other items present a real danger of over-criminalisation.'[9]

Expanding the definition under the ASIO Act to include networks makes it similarly broad. A network may be as small and transient as two mobile phones connected temporarily via Bluetooth to share files between them. A network may also be as a large and permanent as the Internet. ATMs and self-service checkout machines are by their nature networked devices.

Such an expansive definition would seemingly incorporate any individual device and any other device to which it had been connected, with no explanation of whether that should include temporary networks (increasingly common) or larger permanent networks (as found in office buildings, educational institutions, and of course Parliament House). The explanatory memorandum is not helpful for understanding the intention of what is to be included.

This is particularly important given the amendments to section 25A proposed in schedule 2 item 18. The explanatory memorandum states these will 'enable the target computer of a computer access warrant to extend to all computers at a specified location and all computers associated with a specified person.'[10] These amendments allow access to a target computer where 'target computer' includes any or all of the following: a particular computer, a computer on particular premises, and a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

As has been demonstrated above, the definition of 'computer' in this context is unclear, and this may authorise access to more devices than actually intended.

It is doubtful that this approach has been prepared with adequate consultation with information technology experts. The Committee should insist on a more specific, technically-sound definition that reflects the intention of the legislation. There is no indication of how confined or expansive powers relating to computer access are intended to be.

[8] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2010) 52–56.
[9] Ibid 53.
[10] Explanatory Memorandum, National Security Legislation Amendment Bill (No 1) 2014 (Cth) 7.

4 Increased flexibility without increased oversight

There are at least two areas which are identified as examples where flexibility has been increased to the detriment of oversight. Due to time constraints, thorough consideration of this issue has not been possible.

The first is allowing the use of listening, optical surveillance and tracking devices without a warrant. Any use of surveillance powers without a warrant is objectionable: oversight is a must when it comes to intruding upon privacy. If a convincing case cannot be made in order to obtain a warrant, the surveillance should not be permitted. There is significant concern that powers, if unchecked, will be abused. This is a legitimate and undeniable concern: corruption and abuse of powers are things to be avoided and a warrant system significantly increases oversight to mitigate such risks. As an example of the very real threat corruption and abuse of power pose, in July 2014 it was reported that an Australian Federal Police officer had been charged with corruption, including 'unauthorised access to data held in a computer with intent to commit a serious Commonwealth offence [abuse of public office, contrary to subsection 142.2 of the Criminal Code Act 1995], contrary to subsection 477.1 of the Criminal Code Act 1995.'[11] The Committee should not allow this amendment to be made.

A similar concern is raised by amendments proposed in schedule 2 item 8 which allow the ASIO Director-General to authorise a class of persons to execute a warrant. While this is recognised as desirable in some ways for flexibility of execution, no convincing case is made out for its necessity. In the 35 years the ASIO Act has been in force, this does not appear to have raised any significant concerns previously. It is preferably to have a system that clearly confers warrant powers on specific individuals. This is a healthy safeguard against administrative errors and allows easy identification of who may execute a warrant. It is preferable to have specific persons execute a warrant than a potentially broad class.

The Bill should be revised to remove these amendments.

[11] 'Australian Federal Police officer charged with corruption', *News.com.au* (online) 17 July 2014, <http://www.news.com.au/national/australian-federal-police-officer-charged-with-corruption/story-fncynjr2-1226991897404>.

5 Authorising the use of force

In a 2013 Report the Committee recommended

> that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.[12]

Despite this recommendation, among the proposed amendments in schedule 2 items 9 and 41 are provisions *requiring* the authorisation of force against persons in regard to surveillance device warrants and identified persons warrants.

Force against a person *should not* be necessary to execute a surveillance warrant, and this amendment appears to go against the recommendations of the Committee, as well as the convincing argument put forward by the Human Rights Law Centre that

> The Government's proposal to allow ASIO to use reasonable force at any time during the execution of a warrant, not just on entry, may raise concerns in relation to the right of liberty and security of person, which is enshrined in article 9 of the ICCPR.[13]

6 Evidentiary certificates

Evidentiary certificates should be approached with caution given the facts they assert are done so essentially on the guarantee of the organisation wishing to assert the facts they state. The purpose of introducing evidentiary certificates is understood to be an avoidance of exposing operatives and operational methods used to acquire particular evidence.

The explanatory memorandum states that an evidentiary 'certificate

[12] Joint Standing Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) 130.

[13] Human Rights Law Centre, Submission No 140 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms of Australia's National Security Legislation*, 8.

creates a rebuttable presumption as to the existence of the facts contained in the certificate.'[14] Given the wide range of operational matters a certificate may assert, and the covert nature of information gathering, it would be helpful to have some indication of how a defendant would be able to challenge those assertions. In circumstances where the defendant wishes to challenge the means by which evidence was gathered against them, how would they go about this? In the event that they do not have evidence to the contrary, is the evidentiary certificate still assumed to be correct or would the prosecution be required to demonstrate that the certificate is in fact accurate? If it were upheld despite objection, this could be an unscientific approach and would lead to dogma-based prosecution. If, on the other hand, a defendant merely needed to raise doubts about the accuracy of the certificate, this would seemingly undo the purpose of the system by requiring the prosecution to provide evidence as to the accuracy of the certificate and thus potentially revealing the information it sought to conceal.

That being said, it is agreed that evidentiary certificates should not be used to prove material facts. This is in line with the comments of the Committee 'that evidentiary certificates could be used to prove the validity of how information was obtained, but not whether the information itself is true.'[15]

7 The cumulative effect of amendments

There are grave concerns about the cumulative effect of certain amendments, namely:

- Powers contained in schedule 2 to 'add, copy, delete or alter other data' with regard to computers and communications in transit,
- Amendments to warrants in schedule 2 allowing a warrant to cover a network of computers with no restriction on the definition or bounds of a 'network', and
- The ability conferred under schedule 2 to essentially allow access to any other network or computer that would assist in accessing a target computer, and to add, copy, delete or alter data on that third-party computer.

[14] Explanatory Memorandum, National Security Legislation Amendment Bill (No 1) 2014 (Cth) 20.

[15] Joint Standing Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (2013) 131.

The cumulative effect of these three amendments allows ASIO to perform broad, sweeping surveillance of the Internet under a single warrant. Operatives could legally introduce software viruses and network worms across a potentially unlimited number of computers, as long as no interference with the normal use of the computer occurs.

These powers are unnecessarily broad and open to rife abuse. In combination with an evidentiary certificate system, the use of these extraodinarily wide powers can be verified as appropriate by the Director-General and no one would know.

The Committee must recommend against the Bill on the grounds that it would confer far too much discretionary power on an organisation that is already exempt from many checks and balances.

8 Closing remarks

It is recognised that significant concessions to transparency are necessary to protect national security. It is on this basis that intelligence organisations are exempt from legislation such as the *Freedom of Information Act 1982*. Despite this, 'national security' should not be used to justify increases in power while reducing vital checks and balances.

The National Security Legislation Amendment Bill (No 1) 2014 significantly increases the powers of the Australian Security Intelligence Organisation and provides the organisation with substantially greater operational flexibility.

However, this comes at an enormous cost to civil society and fundamental freedoms. The Pirate Party has identified in this submission several significant concerns with this Bill:

- The Bill covers an inappropriately wide number of areas and the proposed amendments should not be contained in a single bill.
- The time given for the public and interested persons and organisations to submit was insufficient for a bill of this magnitude.
- Certain important provisions are placed between less significant amendments, making the Bill deceptive in its scope.
- The Bill may have significant impacts on freedom of political communication by limiting discussion of national security issues and significantly increases penalties for external disclosures.
- Certain provisions increase the opacity of ASIO, an organisation

already exempt from transparency-promoting legislation.
- The definition of 'computer' is intended to be expanded and increases the ambiguity of the term.
- The definition of 'computer' is already broad and will be significantly broadened by these amendments.
- It is unclear what is intended by expanding the definition of 'computer' to include 'networks.'
- The Bill substantially reduces warrant requirements in relation to the use of surveillence devices.
- The Bill reduces the requirements for who may execute certain warrants.
- The Bill requires the authorisation of force against persons in regard to certain warrants, seemingly in contradiction to the Committee's 2013 report.
- The proposed evidentiary certificate system raises concerns for how a defendant would rebut the veracity of the certificate.
- The cumulative effects of amendments relating to computer access give ASIO inappropriately broad powers.

Pirate Party Australia therefore urges the Committee to reject the National Security Legislation Amendment Bill (No 1) 2014, and to recommend that the development of national security legislation be a significantly more participative process with genuine consultation from the public, interested persons and organisations, and experts in the relevant fields.

9 Appendices

A Open letter to the Committee Secretary

Dear Secretary of the Parliamentary Joint Committee on Intelligence and Security,

Pirate Party Australia believes in considered, deliberative and consultative policy development. Our internal procedures are perfectly in line with these ideals, and our policy development is open to all members, and even interested outsiders. Our policies, as they are developed, are open for discussion typically for months before they are considered to be enacted.

It is with this in mind that we are disheartened by the extreme swiftness with which some very serious legislation that potentially affects all Australians is being rushed through the review process.

The time given to respond to the National Security Legislation Amendment Bill (No 1) 2014 is insufficient given the serious and substantial nature of the proposed amendments. It was referred to the Committee on 16 July 2014, with a deadline of 1 August 2014 for submissions on a bill that is 124 pages in length accompanied by an explanatory memorandum of 167 pages.

Although based on prior recommendations the Committee made in its 2013 Inquiry into potential reforms of National Security Legislation, the bill exceeds those recommendations significantly in places. More time is necessary to sufficiently analyse and put forward a measured and reasonable position on these matters.

For example, in a densely worded change to section 18(2) of the Australian Security Intelligence Act 1979, there is a small amendment that could result in far-reaching implications for how far political communication would be restricted.

Without adequate time to analyse all the elements of this extremely long and dense documentation, and to formulate coherent feedback, the process of consultation that is being undertaken would be ineffective, and would result in the process being seen to be a mockery.

We request that, at the very least, a further fourteen (14) days are

granted to all persons and organisations who intend to submit to this committee. To not allow this would be an affront to democracy.

—
Regards,

Mozart Olbrycht-Palmer
Deputy Secretary
Pirate Party Australia