Australian Human Rights Commission

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

AUSTRALIAN HUMAN RIGHTS COMMISSION SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

21 August 2014

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

Table of Contents

1 Introduction

1. The Australian Human Rights Commission (Commission) makes this submission to the Parliamentary Joint Committee on Security and Intelligence in its Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014 (the Bill).

2. The Commission is established by the *Australian Human Rights Commission Act 1986* (Cth) and is Australia's national human rights institution.

3. This submission addresses the potential impact of the Bill on human rights and in particular the rights to privacy and freedom of expression. These rights, reflected in articles 17 and 19 of the *International Covenant on Civil and Political Rights* (ICCPR),[1] may be limited by proportionate measures to achieve a legitimate aim, if protected by safeguards and oversight.

4. Given the short timeframe of the current inquiry, the Commission has focused on those measures of the Bill that raise the most significant human rights concerns and which require further consideration prior to enactment. We have also offered a range of suggestions to ensure that any new measures are accompanied by appropriate safeguards to protect human rights, including the rights to privacy and freedom of expression. The Commission reserves the right to provide further commentary on other elements of the Bill once it has provided more detailed consideration of the Bill.

5. The Commission supports the passage of the Bill, subject to a number of recommendations which address these significant concerns about the Bill's impact on human rights.

2 Summary

6. The Bill seeks to reform existing security legislation in seven key areas:

   - Modernising ASIO's statutory employment framework (Schedule 1)
   - Modernising and streamlining ASIO's warrant-based intelligence collection powers (Schedule 2)
   - Strengthening ASIO's capability to conduct covert intelligence operations, with appropriate safeguards and oversight (Schedule 3)
   - Clarifying and improving the statutory framework for ASIO's co-operative and information sharing activities (Schedule 4)
   - Enhancing the capabilities of intelligence agencies (Schedule 5)
   - Improving the protection of intelligence-related information (Schedule 6) and

- Renaming of Defence agencies to better reflect their roles (Schedule 7).

7. The principal matters dealt with in this submission relate to proposed amendments to the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) and the *Intelligence Services Act 2001* (Cth) (IS Act). These amendments relate to the following intelligence agencies:

   a. The Australian Security and Intelligence Organisation (ASIO)

   b. The Australian Secret Intelligence Service (ASIS)

   c. The Defence Imagery and Geospatial Organisation (DIGO)

   d. The Defence Intelligence Organisation (DIO)

   e. The Defence Signals Directorate (DSD) and

   f. The Office of National Assessments (ONA).

8. The Commission acknowledges the critical importance of ensuring that our security agencies have appropriate powers to protect our national security. Human rights law provides significant scope for such agencies to have expansive powers, even where they impinge on individual rights and freedoms. Such limitations must, however, be clearly expressed, unambiguous in their terms, and legitimate and proportionate responses to potential harms.

9. The Commission considers that in several instances, the Bill goes beyond what can be reasonably justified. We make 10 recommendations to address concern about risk to human rights. The Commission supports the passage of the Bill providing that these recommendations are adopted and the Bill amended accordingly.

3 Recommendations

10. The Australian Human Rights Commission recommends that:

Recommendation 1: Proposed s 25(4)(ab) of the ASIO Act be amended to read 'if having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is *necessary* in all the circumstances to do so *and having regard to the rights of individuals to privacy*…*'*

Recommendation 2: Proposed s 25(6) and s 25A(5) of the ASIO Act be amended so that only minor or inconsequential (or immaterial) interference with computers is permitted in all circumstances.

Recommendation 3: Proposed amendments to s 25, s 25A and proposed sub-ss 26B(1)(g), (2)(c) and (3)(d) of the ASIO Act be clarified so that entering and exiting third party premises is permitted only where it is necessary to execute a warrant.

Recommendation 4: The SIO framework be amended in line with the controlled operations certificate framework in the *Crimes Act 1914* so that the maximum duration of an authority is reduced to 3 months with the possibility of renewal in 3 month increments, (up to a total of 12 months). An independent body should be charged with the decision to renew or issue subsequent authorities.

Recommendation 5: Proposed s 35K of the ASIO Act be amended so that it is a condition of the immunity that the special intelligence conduct was necessary having regard to other means of obtaining the information.

Recommendation 6: The Bill be amended to include a mandatory review of the SIO scheme after 5 years.

Recommendation 7: Proposed s 35P(1) of the ASIO Act be amended so that it is an offence for a person to disclose information where the information relates to a SIO and disclosure of the information *is likely to* endanger the health or safety of any person or prejudice the effective conduct of a SIO.

Recommendation 8: Item 5 of Schedule 4 not be passed. Any alternative provisions should:

a. limit the purposes for which personal information is divulged to private persons and bodies; and

b. restrict any misuse or release of such information by those persons and bodies.

Recommendation 9: Items 1, 6 and 7 of Schedule 5 of the Bill be amended to:

a. clarify the meaning of ‘operational security of ASIS’

b. make clear that the Minister may authorise ASIS to produce intelligence on Australian persons only for the purpose of protecting national security.

Recommendation 10: Schedule 6 of the Bill not be passed. In the event that this recommendation is not accepted, the Commission recommends that Schedule 6 be amended to:

a. provide a defence where the public interest in a disclosure, dealing, or recording outweighs the harm that results from that act

b. provide a defence in circumstances where the relevant information is already in the public domain, but the Commonwealth has not authorised any prior release

c. exclude disclosures, dealings and recordings of information that do not relate to national security

d. provide for a series of gradated offences, where maximum penalties are available only in the case of aggravated offences, in circumstances where:

    i. The information or record disclosed, dealt with, or recorded relates to national security

    ii. The disclosure, dealing, or recording is done with the intention of causing serious harm to national security, and does cause such harm.

4 Human Rights Framework

11. This submission primarily addresses the human rights implications of the Bill arising under articles 17 and 19 of the *International Covenant on Civil and Political Rights* (ICCPR).

4.1 Article 17 – the Right to Privacy

12. Article 17 of the ICCPR provides:

    1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

    2. Everyone has the right to the protection of the law against such interference or attacks.

13. Article 17 protects communications that are made in private. It also protects individuals from the collection of their personal information by others, including government. The HRC has stated:

> [T]he competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant.[2]

14. The HRC has concluded that electronic surveillance (of both content and metadata) will amount to a *prima facie* interference with privacy:

> [A]ny capture of communications data is potentially an interference with privacy and, further… the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.[3]

15. Any limitation on privacy must be lawful. That means that any limitations on the right must be provided for by law.

> Relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such

> authorised interference must be made only by the authority designated under the law, and on a case-by-case basis.[4]

16. Laws must be precise and clear enough to allow individuals to regulate their conduct, and should provide effective remedies in the case of abuse.[5]

17. Further, any interference with the right to privacy must not be arbitrary. The expression 'arbitrary interference' means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances.[6] Reasonable in this context means any limitation must be proportionate and necessary to achieve a legitimate objective.[7] The Office of the High Commissioner for Human Rights has recently stated:

> The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.[8]

4.2 Article 19 – Freedom of Expression

18. Article 19 of the ICCPR provides:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

19. Freedom of expression is both 'an indispensable condition for the full development of the person' and 'a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights.'[9]

20. The only permissible restrictions on the freedom of expression are those described in paragraph 3 of Article 19.[10]

21. Any limitation on the freedom of expression must be according to law. Laws limiting the freedom must be made accessible to the public, and must provide sufficient guidance both to those executing the laws, and to those whose conduct is being regulated.[11]

22. Further, any limitation on the freedom of expression must be necessary and proportionate to achieve a legitimate objective. The objective must be one within the scope of article 19(3). The means adopted to achieve it must not destroy the essence of the right. It is for a State party to the ICCPR to demonstrate the legal basis for any restriction on the freedom.[12]

23. Article 19 expressly contemplates that the freedom of expression may be limited for the protection of national security. The term 'national security' refers to the protection of the existence of a nation. The *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (Siracusa Principles)[13] state:

> 29. National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.
>
> 30. National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order.
>
> 31. National security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse.

24. The Siracusa Principles go on to observe that the systematic violation of human rights undermines 'true national security'.[14]

25. The HRC has made similar comments in General Comment 34:

> Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3 [of article 19]. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. Nor is it generally appropriate to include in the remit of such laws such categories of information as those relating to the commercial sector, banking and scientific progress.[15]

26. Article 19(3) provides for a number of other limitations on the freedom of expression, including the protection of the rights of others. The rights relevant to this limitation include 'human rights as recognised in the [ICCPR], and more generally in international human rights law.'[16]

27. It should be noted that article 19 includes a right to have access to information. It therefore requires that appropriate protection be afforded to

whistleblowers. This issue has received particular attention from international experts in the field of secrecy laws enacted in the name of national security.

28. For instance, the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information* include the following:[17]

> **Principle 12: Narrow Designation of Security Exemption**
> A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.
>
> **Principle 13: Public Interest in Disclosure**
> In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.
>
> ….
>
> **Principle 15: General Rule on Disclosure of Secret Information**
> No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.
>
> **Principle 16: Information Obtained Through Public Service**
> No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.
>
> **Principle 17: Information in the Public Domain**
> Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.

29. The *Global Principles of National Security and the Right to Information* (Tshwane Principles) contain similar provisions.[18] For instance, they provide that certain types of disclosure should be protected, including those which reveal corruption or human rights violations.[19]

30. Consistently with these principles, the UN High Commissioner for Human Rights has recently stated that whistleblowers who disclose human rights violations should be protected.[20]

5 Schedule 2: Expanding warrant powers

5.1 Extending the definition of computer

31. Under existing s 25A of the ASIO Act, the Minister may issue a computer access warrant. The Commission notes that the Bill will amend the definition of computer in s 22 to mean all or part of (a) one or more computers; or (b) one or more computer systems; or (c) one or more computer networks; or (d) any combination of these.

32. Item 18 of Schedule 2 of the Bill amends s 25A to 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.

5.2 Access via third party computers and communications

33. The Bill inserts new s 25A(4)(ab) into the ASIO Act, which enables the use of a third party computer or communication in transit (and to 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 held on the target computer.

34. The proposed provision contains the legislative safeguard that this may only be done 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.

35. Accessing third party computers, where the individuals are not a direct threat to security in order to gain access to the target computer is a potentially broad power. As acknowledged by the Bill's Statement of Compatibility with Human Rights, it restricts the right to privacy contained in article 17 of the ICCPR.[21]

36. In order to better protect against arbitrary interferences of privacy, the Commission recommends that the legislative safeguard instead read **'necessary'** in the circumstances having regard to other methods of obtaining access to the data which are likely to be as effective 'and having regard to the rights of individuals to privacy'.

Recommendation 1: Proposed s 25(4)(ab) of the ASIO Act be amended to read 'if having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is *necessary* in all the circumstances to do so *and having regard to the rights of individuals to privacy…'*

5.3 Enabling the disruption of the target computer

37. The Bill also amends the computer disruption limitations currently contained in s25(6) and s25A(5) of the ASIO Act. Currently s 25(6) and s 25A(5) of the ASIO Act do not authorise the addition, deletion or alteration of data, or the doing of any thing that interferes with, interrupts or obstructs the lawful use by other persons of a computer or other electronic equipment or a data storage device, found on the subject premises or that causes any loss or damage to other persons lawfully using the computer, equipment or device.

38. In its *Report of the Inquiry into Potential Reform of Australia's National Security Intelligence Legislation*, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) noted that this prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be.[22] The existing formulation apparently led to difficulties in executing computer access warrants.[23]

39. Proposed s 25(6) and s 25A(5) of the ASIO Act provide that (the warrant) does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to:

    a. materially interfere with, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises unless the addition, deletion or alteration or the doing of the thing, is necessary to do one or more of the things specified (in the warrant)

    b. cause any other material loss or damage to other persons lawfully using the computer, equipment or device.[24]

40. The provision authorises the addition, deletion or alteration of data that is likely *to materially* interfere with the lawful use of the computer or device by other persons where it is necessary to carry out the warrant. In light of the extension of the definition of computer, this amendment has the capacity to enable ASIO employees to interfere with entire computer networks in a material way where it is necessary to execute the warrant. As noted by the Bill's Statement of Compatibility with Human Rights, the proposed provision restricts the right to privacy in article 17 of the ICCPR.[25]

41. Justification for the provisions was based on the problems caused by not being able to make minor and inconsequential interferences. The Commission therefore considers that allowing *material* interference that is necessary to execute the warrant is not proportionate to the legitimate aim of gathering security intelligence.

    Recommendation 2: Proposed s 25(6) and s 25A(5) of the ASIO Act be amended so that only minor or inconsequential (or immaterial) interference with computers is permitted in all circumstances.

5.4 Third party premises

42. The Bill amends s 25, 25A of the ASIO Act and inserts new s 26B(1)(g), (2)(c), (3)(d) to clarify that search warrants, computer access warrants and surveillance device warrants authorise access to third party premises for the purposes of gaining entry to or exiting the subject premises.

43. The entry into innocent persons' homes infringes the right to privacy in article 17 of the ICCPR. To avoid being arbitrary, such entry should be justified and proportionate to the national security purpose. In order to restrict this power to that which is justified and proportionate, entering third party premises should be limited to cases where it is necessary to execute the warrant having regard to other means of executing the warrant.

    Recommendation 3: Proposed amendments to s 25, s 25A and proposed sub-ss 26B(1)(g), (2)(c) and (3)(d) of the ASIO Act be clarified so that entering and exiting third party premises is permitted only where it is necessary to execute a warrant.

6 Schedule 3: Special Intelligence Operations

6.1 Special intelligence operations framework

44. Schedule 3 of the Bill implements the Government's response to Recommendation 28 of the PJCIS's Report by amending Part III of the ASIO Act to insert a new Division 4, which establishes a statutory framework for the conduct by ASIO of special intelligence operations (SIOs).

45. The explanatory memorandum states that a legislative framework for the conduct of SIOs is necessary to ensure that ASIO employees and affiliates will have appropriate legal protection if it is necessary to engage in authorised, covert activities and operations that involve otherwise unlawful conduct for the legitimate purpose of carrying out functions in accordance with the ASIO Act.[26] The establishment of a statutory immunity removes the possibility that conduct in accordance with an authorised SIO could be investigated or referred for prosecution.

46. The Commission acknowledges that an immunity framework may be necessary for the effective conduct of ASIO investigations. However, the immunity framework should be appropriately targeted to conduct that is necessary in authorised activities for the purpose of carrying out the functions of the ASIO Act.

47. Section 4 defines a SIO to be an operation:

    a. in relation to which a special intelligence authority has been granted; and

    b. that is carried out for a purpose relevant to the performance of one or more special intelligence functions; and

    c. that may involve an ASIO employee or an ASIO affiliate in special intelligence conduct.

48. Section 4 defines 'special intelligence function' to mean specific functions of ASIO under s 17(1) of the ASIO Act including to obtain, correlate and evaluate intelligence relevant to security.

49. 'Special intelligence conduct' is defined by s 4 of the ASIO Act to mean conduct for or in relation to which a person would, but for s 35K, be subject to civil or criminal liability under a law of the Commonwealth, a State or a Territory.

50. The Director-General or Deputy Director-General may grant a special intelligence authority. Under proposed s 35C the issuing criteria include that:

    a. the SIO will assist ASIO in the performance of one or more special intelligence functions

    b. that the circumstances justify the conduct specified

c. that the SIO will limit unlawful conduct to the maximum extent possible

d. that the SIO will not be conducted in such a way that a person is likely to be induced to commit an offence that the person would not otherwise have intended to commit, and

e. the conduct will not cause death or serious injury to any person, or involve the commission of a sexual offence, or result in significant loss of property or serious damage to property.

51. The maximum duration for a SIO authority is 12 months. The Commission notes that under s 15GK(1) of the *Crimes Act 1914* (Cth), a controlled operation certificate lasts only three months unless it is renewed in three month increments (up to a total of 24 months). Further, a nominated Administrative Appeals Tribunal member makes the decision whether to renew a controlled operations certificate.[27] This is an important safeguard against the possibility of rolling controlled operation certificates.

Recommendation 4: The SIO framework be amended in line with the controlled operations certificate framework in the *Crimes Act 1914* so that the maximum duration of an authority is reduced to 3 months with the possibility of renewal in 3 month increments, (up to a total of 12 months). An independent body should be charged with the decision to renew or issue subsequent authorities.

52. Proposed s 35K of the ASIO Act provides immunity from liability for special intelligence conduct during SIOs provided a number of conditions are satisfied. Importantly the conditions do not include that the special intelligence conduct was necessary and there were no other means of obtaining the security information.

Recommendation 5: Proposed s 35K of the ASIO Act be amended so that it is a condition of the immunity that the special intelligence conduct was necessary having regard to other means of obtaining the information.

53. Further, as this is a new and exceptional scheme, the Commission considers it important that the Bill contain a mandatory review after 5 years.

Recommendation 6: The Bill be amended to include a mandatory review of the SIO scheme after 5 years.

6.2 New disclosure of information offences

54. Schedule 3 of the Bill also creates two new offences, one being an aggravated offence, in relation to the unauthorised disclosure of information relating to a SIO.

55. The first offence in proposed section 35P(1) of the ASIO Act creates an offence punishable by imprisonment for 5 years for ‘a person’ to disclose information where the information *relates to* a SIO.

56. The second aggravated offence is in proposed s 35P(2) of the ASIO Act. The relevant aggravating elements are that:

    a. in disclosing the information, the person intends to endanger health or safety of any person or prejudice the effective conduct of a SIO, or

    b. the disclosure of information will endanger the health and safety of any person or prejudice the effective conduct of a special intelligence operation.

57. The new offences contain some defences – including disclosures pertaining to the operation of the SIO scheme or legal proceedings relating to Division 4 of the ASIO Act, other legal obligations of disclosure and disclosures for the purpose of the performance by ASIO of its statutory functions.

58. As the provisions deal with disclosures from 'a person', they have the potential to capture the work of journalists and potentially limit the right to freedom of expression under article 19 of the ICCPR. The HRC has stated that:

> the media plays a crucial role in informing the public about acts of terrorism and its capacity to operate should not be unduly restricted. In this regard, journalists should not be penalized for carrying out their legitimate activities.[28]

59. The explanatory memorandum states that these offences are necessary to protect persons participating in a SIO and to ensure the integrity of operations, by creating a deterrent to unauthorised disclosures, which may place at risk the safety of participants or the effective conduct of the operation.[29] This is a legitimate ground for restriction of freedom of expression.

60. The HRC has stated that when a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in a specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.[30]

61. The ordinary offence punishable by 5 years imprisonment appears to apply to past as well as present SIOs and regardless of whether it will endanger the health and safety of a person or prejudice the effective conduct of a SIO. It will capture journalists publishing information *relating to* a SIO. Journalists and others may not even know that a SIO has been authorised. In the Commission's view there is not a sufficient, direct and immediate connection between the limitation on expression and the threat.

62. The Commission recommends that the offence punishable by 5 years' imprisonment be amended so that it prohibits disclosure of information relating to a SIO *that is likely to* endanger health or safety of any person or prejudice the effective conduct of a SIO.

63. The Commission notes that such an amendment would not affect the provision in s35P2 which relates to mores serious situations where there is intent to cause danger.

Recommendation 7: Proposed s 35P(1) of the ASIO Act be amended so that it is an offence for a person to disclose information where the information relates to a SIO and disclosure of the information *is likely to* endanger the health or safety of any person or prejudice the effective conduct of a SIO.

7 Schedule 4: Co-operation and Information Sharing

64. Section 19(1) of the ASIO Act currently allows ASIO to co-operate with:

    - authorities of the Commonwealth
    - Departments, Police Forces and authorities of the States, and
    - authorities of other countries approved by the relevant Minister as being capable of assisting the Organisation in the performance of its functions.

65. Item 5 of Schedule 4 of the Bill seeks to amend s 19(1) of the ASIO Act to allow ASIO to co-operate with any person or body, either inside or outside Australia, in the performance of its functions. The Statement of Compatibility with Human Rights states that this is merely a 'confirmation' of the current powers of ASIO and reflects ASIO's current practice.[31]

66. The Explanatory Memorandum states that the ability to co-operate is important, inter alia, because the private sector owns much of Australia's critical infrastructure.[32] It goes on to say that ASIO's engagement with private entities:

> seeks to enable Australian business security managers to recognise and respond to national security related threats, develop and implement appropriate risk management strategies and provide informed briefings to executives and staff.[33]

67. The ambit of the 'co-operation' envisaged by this amendment is not clear. However, the Statement of Compatibility with Human Rights makes clear that co-operation may involve the sharing of personal information by ASIO.[34] It is thus apparent that this provision would to some extent restrict the right to privacy contained in article 17.

68. The only limit on ASIO's ability to co-operate with others will be that that co-operation must be 'necessary for, or conducive to', ASIO's functions.[35]

69. The Commission notes that as it stands, s 19 allows co-operation with a very limited and defined range of entities, all of which are governmental organs or authorities. Government agencies are likely to be accountable in ways that private entities are not. Further, ASIO may only co-operate with foreign governments with the consent of the Minister.

70. The proposed amendment would potentially allow ASIO to co-operate with private entities, including foreign ones, with fewer restrictions than apply to it when co-operating with foreign governments.

71. As the Explanatory Memorandum points out, ASIO's co-operation with entities under s 19 of the ASIO Act may be subject to arrangements made or directions given by the Minister under subsection 19(1) of that Act. The Minister may also give relevant directions under s 8A. However, there is no requirement that any such arrangements or directions be made.

72. Section 18(2) of the ASIO Act makes it an offence for persons to make a communication of any information received from ASIO if they have received it 'having entered into any contract, agreement or arrangement' with ASIO. However, it is not clear that all co-operation between ASIO and a person or body, under which ASIO might communicate personal information about third parties, would necessarily occur under a 'contract, agreement or arrangement' for the purposes of s 18(2).

73. The Commission is concerned that this amendment would allow ASIO to share sensitive personal information with any person or organisation it chose, with very little recourse in the event that person or organisation subsequently misused or released the information.

74. As noted above, for a restriction on the right to privacy to be legitimate, the Government must demonstrate that it is necessary and proportionate to achieve a legitimate end. In bestowing such a wide power to share personal information on ASIO, with little control about the purposes for which it is shared or measures to ensure it is not misused or released, the Bill appears to go beyond what is necessary and proportionate to achieve its goals.

Recommendation 8: Item 5 of Schedule 4 not be passed. Any alternative provisions should:

a. limit the purposes for which personal information is divulged to private persons and bodies; and

b. restrict any misuse or release of such information by those persons and bodies.

8 Schedule 5: Activities and Functions of *Intelligence Services Act 2001* Agencies

75. Under the IS Act, ASIS is able, in certain circumstances, to collect information about Australian persons. These circumstances are limited. In particular, ASIS cannot undertake activities with the specific aim of producing intelligence on Australians unless it is authorised to do so by the relevant Minister.[36] Before the Minister can give such authorisation, he or she must be satisfied that one of a limited range of circumstances exists, such as the presence of a threat to security.[37]

76. Item 6 of Schedule 5 of the Bill proposes to amend s 9(1A)(a) of the IS Act to include a new ground on which the Minister may authorise ASIS to produce intelligence about Australians. That ground is that the Minister is satisfied that the person is, or is likely to be, involved in activities that do or are likely to pose a risk to the 'operational security' of ASIS.

77. Item 1 of Schedule 5 seeks to insert the following definition of 'operational security' into the IS Act:

> ***operational security of ASIS*** *means the protection of the integrity of operations undertaken by ASIS from:*
>
> *(a) interference by a foreign person or entity; or*
>
> *(b) reliance on inaccurate or false information.*

78. As the Statement of Compatibility with Human Rights acknowledges, the production of intelligence about a person necessarily involves a restriction on that person's right to privacy under article 17 of the ICCPR.[38]

79. The Australian government is required to respect the right to privacy of all those within its jurisdiction. In the field of covert intelligence gathering, that includes non-citizens who may come under surveillance by Australian authorities.[39]

80. The Commission has two concerns about expanding the grounds on which the Minister may authorise ASIS to deliberately produce intelligence on Australians in this way.

81. First, it is not entirely clear what kinds of conduct or potential conduct would satisfy the requirements of the new definition of 'operational security.' The amendments would allow the Minister to authorise ASIS to produce intelligence about a person if that person is likely to be involved in activities which are likely to pose a risk to the protection of the integrity of ASIS's operations from reliance on inaccurate information. The concept of 'a risk to the protection of…' is particularly unclear.

82. The Explanatory Memorandum indicates that the purposes of the amendment include the protection of the integrity of ASIS' operations 'where ASIS is at risk of relying on inaccurate or false information'.[40] If the intention is to allow ASIS to be authorised to produce intelligence about Australians in all circumstances where to do so would reduce the risk that ASIS would rely on inaccurate information, the provision might well be seen to allow authorisation of the production of intelligence in *any* circumstances, as further intelligence will presumably *always* reduce the risk of false information being relied on.

83. On the other hand, the Commission notes that the amendment requires that a person must be engaged in (or be likely to engage in) an 'activity' which is linked to the relevant risk. If the intention of the amendment is to allow ASIS to produce intelligence on persons engaged in activities designed to deliberately induce ASIS to rely on false information, the provisions should be amended to better capture that intention.

84. The Commission's second concern relates to the justification given for expanding ASIS's power to produce intelligence on Australians.

85. The Statement of Compatibility states that the proposed amendment:

> is for a legitimate objective – to assist ASIS in performing its existing function of conducting counter-intelligence under the IS Act. The limitation is authorised by law and is consistent with the objectives of the ICCPR, which include State sovereignty and protection of the nation state, including national security.[41]

86. Conducting 'counter-intelligence' is not in itself a legitimate objective to limit the rights contained in article 17. Conducting counter-intelligence to protect national security could be a legitimate objective. However, the proposed amendment goes beyond protecting national security. That is because ASIS' functions are not limited to the protection of national security. Section 11 of the IS Act provides that the functions of relevant intelligence agencies, including ASIS:

> are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

87. The Explanatory Memorandum expressly indicates that the amendment will allow ASIS to produce intelligence relating to matters that do not implicate "security" within the meaning of the ASIO Act.[42]

88. These matters appear likely to go beyond factors that could justify the serious restriction on the right to privacy entailed by producing intelligence on an individual. The government bears the onus of demonstrating that a restriction on the right to privacy is justified. The Commission considers that the government has not provided an adequate justification for these proposed amendments.

Recommendation 9: Items 1, 6 and 7 of Schedule 5 of the Bill be amended to:

a. clarify the meaning of 'operational security of ASIS'

b. make clear that the Minister may authorise ASIS to produce intelligence on Australian persons only for the purpose of protecting national security.

9 Schedule 6: Protection of Information

89. Schedule 6 of the Bill seeks to amend several provisions of the ASIO Act and the IS Act which make it illegal for employees, agents and contractors of ASIO, ASIS and several other intelligence agencies to communicate without authorisation information gathered by those organisations. It also creates a number of new offences relating to the unauthorised communication, dealing with or recording of information by staff, agents or contractors of various intelligence organisations.

90. Section 18(2) of the ASIO Act currently makes it an offence for an ASIO officer to make:

> 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 [ASIO] 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 by the Organisation of its functions…

unless the person is authorised to make the communication or makes it in accordance with their duties under the ASIO Act.

91. Similar offences exist under the IS Act in relation to the unauthorised communication of information by employees or contractors of ASIS,[43] DIGO,[44] and the DSD.[45] In the case of information relating to ASIO, the current penalty for a breach of s 18(2) is imprisonment for a maximum term of 2 years. In the case of information relating to ASIS, DIGO and the DSD, unlawful communication carries a maximum penalty of 2 years' imprisonment, and/or 120 penalty units.[46]

92. The Bill increases the maximum penalty for all these offences to imprisonment for 10 years.

93. The Bill creates offences in the same terms for the communication of information relating to the ONA and the DIO.[47]

94. The increased penalties for the existing offences, and the penalties for the equivalent newly created offences in relation to the ONA and the DIO, are dramatically greater than those that currently apply. The Explanatory Memorandum states that the increase is required because the current penalties are:

> disproportionate to the significant, adverse consequences that the unauthorised disclosure of highly classified information can have on a country's reputation, intelligence-sharing relationships and intelligence-gathering capabilities. A higher maximum penalty is needed to reflect the gravity of the wrongdoing inherent in such conduct in the contemporary security environment.[48]

95. It goes on to state that this has been demonstrated to be the case by '[r]ecent domestic and international incidents involving the unauthorised communication of security intelligence-related information….'[49] This would appear to be a reference to releases of information made in recent in times in other jurisdictions by persons and organisations such as Chelsea Manning, Edward Snowden and WikiLeaks.

96. As noted above, Article 19 requires that protection be given to certain releases of information even when that may negatively affect national security.

97. The Bill also creates a number of new offences.[50] It makes illegal the unauthorised copying, transcribing, retaining, removing, or dealing in any other manner with certain intelligence agency records by employees or contractors of ASIO, ASIS, DIGO, DIO, DSD and ONA.[51] It also makes illegal

the unauthorised recording of information gathered in the course of working for those organisations. These offences are punishable by a maximum term of imprisonment of 3 years.[52]

98. It is a defence to each of these offences if the relevant record or information has already been communicated or made available to the public with the authority of the Commonwealth.

99. These offences penalise the communication of information and the taking of steps which may lead to the communication of information. They therefore restrict the right to freedom of expression contained in article 19 of the ICCPR. They restrict both the right to impart information and the right to receive it. As the laws relate to information and records relating to national security, they restrict expression about a matter of very significant importance. As discussed above, restrictions on the freedom of expression may be justified by the need to protect national security, but any such restrictions must be necessary and proportionate.

100. The Commission notes that it is not an element of any of the amended or newly created offences that a person intend to cause harm to Australia's interests. Nor is it an element that they *in fact* cause harm to Australia's interests (including its national security). The offences apply with respect to any information relating to a relevant intelligence agency, regardless of whether the information itself is relevant to intelligence or national security. Several of the intelligence agencies have functions that go beyond the protection of national security,[53] and all will necessarily generate some information the release of which could not jeopardise national security. In the case of the new offences of dealing with information and creating records, it is not an element of the offences that any information at all be communicated outside the relevant agency.

101. As noted above, it is a defence to any of the offences if the relevant information has already been made public with the authority of the Commonwealth. However, that defence will not be available if the Commonwealth has not given its authority to release information, even if that information is in the public domain.

102. There is no public interest defence available in relation to any of the offences.

103. The Commission acknowledges that there are mechanisms by which staff of intelligence agencies can, in certain circumstances, make disclosures of information in the public interest. Under the *Public Interest Disclosure Act 2013* (Cth), internal disclosures may be made to the relevant agency or the Inspector-General of Intelligence and Security.[54] That addresses some of the negative practical consequences that could flow from restricting freedom of expression on national security grounds, and provides an avenue by which whistleblowers may be able to make disclosures. It does not, however, address all of the matters identified above.

104. Given all of these factors, the Commission considers that the increases in penalties and the creation of new offences in Schedule 6 of the Bill have not

been demonstrated to be necessary and proportionate to the government's objective of protecting national security.

Recommendation 10: Schedule 6 of the Bill not be passed. In the event that this recommendation is not accepted, the Commission recommends that Schedule 6 be amended to:

a. provide a defence where the public interest in a disclosure, dealing, or recording outweighs the harm that results from that act

b. provide a defence in circumstances where the relevant information is already in the public domain, but the Commonwealth has not authorised any prior release

c. exclude disclosures, dealings and recordings of information that do not relate to national security

d. provide for a series of gradated offences, where maximum penalties are available only in the case of aggravated offences, in circumstances where:

i. the information or record disclosed, dealt with, or recorded relates to national security, and

ii. the disclosure, dealing, or recording is done with the intention of causing serious harm to national security, and does cause such harm.

---

[1] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). At http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (viewed 19 August 2014).
[2] UNHRC, *General Comment 16* (1988), UN Doc. HRI/GEN/1/Rev.1 at 21, [7].
[3] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), [20].
[4] UNHRC, *General Comment 16* (1988) UN Doc. HRI/GEN/1/Rev.1 at 21, [8].
[5] See UNHRC, *Concluding Observations on the United States of America*, (2014) UN Doc. CCPR/C/USA/CO/4, [22].
[6] UNHRC, *General Comment 16* (1988) U.N. Doc. HRI/GEN/1/Rev.1 at 21, [3], [4].
[7] *Toonen v Australia* UN Human Rights Committee Communication No. 488/1992.
[8] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), [23].
[9] UNHRC, *General Comment 34* (2011), UN Doc. CCPR/C/GC/34, [2]-[3].
[10] UNHRC, *General Comment 34*, (2011), UN Doc. CCPR/C/GC/34, [22].
[11] UNHRC, *General Comment 34*, (2011), UN Doc. CCPR/C/GC/34, [25].
[12] UNHRC, *General Comment 34*, (2011), UN Doc. CCPR/C/GC/34, [27].
[13] United Nations Economic and Social Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, U.N. Doc. E/CN.4/1985/4, Annex (1985), [29]-[31].
[14] At [32].
[15] UNHRC, *General Comment 34* (2011), UN Doc. CCPR/C/GC/34, [30].
[16] UNHRC, *General Comment 34* (2011), UN Doc. CCPR/C/GC/34, [28].
[17] *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information* (1996), available at http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf (accessed on 14 August 2014).

[18] *The Global Principles of National Security and the Right to Information* (Tshwane Principles) (2013), available at http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles (accessed on 14 August 2014).
[19] Principle 37.
[20] Navi Pillay, UN High Commissioner for Human Rights, speaking at the launch of Office of the UN High Commissioner for Human Rights publication *The right to privacy in the digital age*, reported at http://www.abc.net.au/news/2014-07-17/snowden-deserves-protection-from-prosecution3a-un-rights-chief/5603236, 17 July 2014 (accessed on 14 August 2014).
[21] Statement of Compatibility with Human Rights, 10 [30].
[22] PJCIS Report, Chapter 4, 89 [4.24].
[23] See Explanatory Memorandum, 67 [252]-[257].
[24] Similar provisions appear in s 27D(7) and s27E(5).
[25] Statement of Compatibility with Human Rights,10 [30]-[31].
[26] Explanatory Memorandum, 15 [55].
[27] *Crimes Act 1914* (Cth), s 15GU.
[28] UN Human Rights Committee *General Comment 34*, [46].
[29] Explanatory Memorandum, 111 [553].
[30] UN Human Rights Committee *General Comment 34*, [35].
[31] At 24 [101].
[32] At 118 [592].
[33] At 118 [592].
[34] At 24 [104].
[35] ASIO Act, s 19.
[36] IS Act, s 8(1)(a)(i)
[37] IS Act, s 9(1A)(a).
[38] Statement of Compatibility with Human Rights, 26 [111].
[39] UNHRC, *Concluding Observations on the United States of America*, (2014) UN Doc. CCPR/C/USA/CO/4, [22].
[40] Explanatory Memorandum, 120 [604].
[41] Statement of Compatibility with Human Rights, 26 [111].
[42] Explanatory Memorandum, 120 [606].
[43] IS Act, s 39.
[44] IS Act, s 39A.
[45] IS Act, s 40.
[46] A penalty unit is currently $170 – *Crimes Act 1914* (Cth), s 4AA.
[47] Schedule 6, Item 18, proposed new ss 40A and 40B.
[48] Explanatory Memorandum, 129 [674].
[49] Explanatory Memorandum, 130 [679].
[50] Proposed new ss 18A and 18B of the ASIO Act and proposed new ss 40A-40M of the IS Act.
[51] As renamed by Schedule 7 of the Bill.
[52] Schedule 6, Item 18, proposed ss 40C-40M.
[53] Se eg IS Act ss 6 and 11 re ASIS; *Office of National Assessments Act 1977* (Cth) s 5.
[54] *Public Interest Disclosure Act 2013* (Cth), s 34.