Human Rights Law Centre

Response to amendments proposed by the Attorney-General's Department

Supplementary submission to the Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

14 March 2018

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Contact

Dr Aruna Sathanapally (Director), **Hannah Ryan** (Lawyer)

Human Rights Law Centre, Sydney

T: + 61 2 8599 2127
E: aruna.sathanapally@hrlc.org.au
W: www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses a strategic combination of legal action, advocacy, research, education and UN engagement to protect and promote human rights in Australia and in Australian activities overseas.

It is an independent and not-for-profit organisation and donations are tax-deductible.

Follow us at http://twitter.com/rightsagenda
Join us at www.facebook.com/HumanRightsLawCentreHRLC/

1. Introduction

1. The Human Rights Law Centre (**HRLC**) has previously made a written submission and given evidence to the Committee as part of its inquiry into the *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (**the Bill**).

2. After consultation with stakeholders, including the HRLC, the Attorney-General's Department has drafted proposed amendments to the Bill. The purpose of this letter is to address those proposed amendments.

3. We support each of these amendments, which improve the Bill and address a number of the concerns regarding Schedule 2 raised in HRLC's previous submission. We welcome the Department's early provision of these amendments to the PJCIS.

4. Nevertheless, even with these amendments, the HRLC maintains significant concerns that the scope of the Bill is such as to disproportionately burden freedom of expression, and curtail the principle of open government in Australia.

5. We strongly recommend that further amendments be made prior to passage of the Bill. We welcome the Attorney-General's continuing openness to further amendments to ensure that the Bill protects government information in a manner that is appropriate in a liberal democracy.

2. Proposed amendments

6. The proposed amendments would change the regime in Schedule 2 in **four** material ways.

2.1 Amended definition of 'cause harm to Australia's interests'

7. The offence in new section 122.2 is a general secrecy offence which incorporates a harm requirement – that is, it takes a harm-based approach. The definition of 'cause harm to Australia's interests' in new section 121.1 sets out the interests protected by the offence in section 122.2.

8. In our previous submission to the Committee, we explained that the list of interests in this definition extended beyond essential public interests to public interests of a lower order that do not warrant the application of criminal sanctions.

9. **The proposed amendments would narrow the list of interests in the definition of '*cause harm to Australia's interests*' in new section 121.1 to only those interests that are appropriately captured within a general secrecy offence** (for the reasons set out in our previous submission). We welcome this proposal.

2.2 Separate offences for non-Commonwealth officers

10. The offences in new sections 122.1, 122.2 and 122.3 of the Bill apply to any person, whether or not that person is a Commonwealth officer.

11. In our previous submission to the Committee, we explained that non-Commonwealth officers ("outsiders") should not be subject to the same offences and penalties as government insiders.

12. **The proposed amendments would limit the application of the offences in new sections 122.1 – 122.3 to current and former Commonwealth officers.** We welcome this proposal.

13. New section 122.4A proposes a separate offence to apply to non-Commonwealth officers.

14. Except in its reliance on security classification in paragraphs (1)(d)(i) and (2)(d)(i), new section 122.4A does adopt harm as an essential element of each offence. We welcome this sensible approach.

15. However, proposed new section 122.4A does not capture an essential element of any secrecy offence that applies to outsiders, being either that the outsider was provided the information on a confidential basis, or that the outsider knew or was reckless as to the fact that the information was disclosed to them in breach of a secrecy offence.

16. Moreover, as set out below, the proposed new offence is not limited to disclosure but extends to "dealing" with information, which includes receipt, possession or making a record. Therefore, it appears that, even with these proposed amendments, the Bill would criminalise innocent receipt of information by a non-Commonwealth officer, if the information has a security classification of secret or above.

17. With respect to the principles to guide the creation of any secrecy offence applying to non-Commonwealth officers, we refer the Committee to the clear guidance in Recommendations 6-6 and 6-7 of the ALRC's report (set out in the Appendix below).

18. We note that new section 122.4A is essentially the general secrecy offence recommended by the ALRC to apply to Commonwealth officers. We would strongly encourage the Committee to look carefully at this new proposal from this perspective.

2.3 Amended definition of 'inherently harmful information'

19. New section 122.1 criminalises communication, dealing with or handing information that is defined as "inherently harmful information".

20. In our previous submission, we raised our serious concerns with this general secrecy offence that applies to broad categories of information, bearing in mind also the very broad definition of "information."

21. The proposed amendments would remove paragraph (d) from the definition of "inherently harmful information" (being "*information that was provided by a person to the Commonwealth or an authority of the Commonwealth in order to comply with an obligation under a law or otherwise by compulsion of law*"). **This is a necessary amendment, and we support the recognition in the proposed amendments that the material that would be captured by paragraph (d) is not appropriate for inclusion in a general secrecy offence.**

22. The proposed amendments would also narrow the meaning of paragraph (a) of the definition of "inherently harmful information" (being "*security classified information*"). Under the Bill, "security classification" is to have the meaning prescribed by regulations. Under the proposed amendments, security classification will mean a classification of secret or top secret, or an equivalent classification or marking prescribed by regulation. The proposed amendments also remove strict liability for offences involving security classified information.

23. **This proposed amendment is a definite improvement on the Bill.** It would remove from the definition of inherently information a very large volume of documentation and communications that are routinely classified as 'protected' and 'confidential' across the entire Commonwealth public service.

24. However, it remains the case that security classification is an administrative system that is not suitable for inclusion as an element in a serious criminal offence, for the reasons outlined in our submission (see paragraphs 86-89).

25. **We reiterate the rule of law concern that arises where future criminal liability is triggered by an administrative classification that is not governed by law, yet forms an element of a serious criminal offence.**

26. If the Committee is minded to accept a role for 'secret' and 'top secret' classifications, as proposed by the Attorney-General, then the Committee should recommend that:

    (a) mandatory guidelines be set out, for instance, in regulations, for the use of these higher-level classifications, setting out the criteria to be met and the oversight applied to classification decisions;

    (b) a legislative requirement be introduced that the security classification be confirmed prior to the institution of any criminal proceedings;

    (c) procedures be instituted for timely declassification;

    (d) measures be introduced to address the documented practice of over-classification.

2.4 Amended defence for persons engaged in the reporting of news

27. New section 122.5 contains a defence for journalists if certain specified conditions are met.

28. In our previous submission, we welcomed the inclusion of this defence, but raised two concerns, one of which was the requirement that a journalist has engaged in "fair and accurate reporting" in addition to having dealt with information in the public interest. We recommended the removal of the requirement in new section 122.5(6)(b).

29. The proposed amendments would make this change, and more broadly, would improve the defence for those engaged in reporting news. We support these amendments to new section 122.5.

30. The second concern we raised was more fundamental – that is, that in order to ensure freedom of expression, and a free press, it is important not only to protect journalists and media staff who report on matters in the public interest, but the sources of information who risk themselves to bring matters of public interest to light.

31. We remain concerned that the Bill does not adequately protect public interest disclosures, see Part 3.3 below.

3. Remaining concerns with Schedule 2 of the Bill

32. The proposed amendments do not address several of the concerns raised in our previous submission, each of which remain significant areas where changes need to be made to the Bill.

3.1 New sections 122.1 and 122.4 do not adopt a harm-based approach

33. Our previous submission set out at length the role of general secrecy offences within a multi-method approach that includes administrative sanctions, specific secrecy offences and robust public interest disclosure processes, based on the sustained attention that has been given to the issue of how to protect sensitive government information in a healthy democracy.

34. Within this multi-method approach, we endorsed a harm-based approach as the best way to ensure that general criminal offences only capture those disclosures that must be prevented for essential public interests. This approach accords with Australia's obligations under international law and was central to the ALRC's recommendations as to how to strike a balance between the competing public interests of protecting Commonwealth information yet maintaining an open and accountable system of government.

35. Accordingly, any proposal for offences such as those in 122.1 and 122.4 must be treated with great caution.

36. New section 122.1, in our view, is not entirely coherent as an offence. While stated to be a provision that criminalises "inherently harmful information", the definition of "inherently harmful information" in turn includes a harm-based test in paragraph (b). It would appear logical for

paragraph (b) to be included instead in the definition of "cause harm to Australia's interests" and thereby included within new section 122.2.

37. We reiterate our concern as to the breadth of information potentially caught in paragraphs (c) and (e) of the definition of "inherently harmful information", particularly given that they include any foreign intelligence agency or foreign law enforcement agency. It is not at all evident that this breadth of information is inherently harmful in the requisite sense for a general secrecy offence. Paragraph (e) remains inconsistent with the principles in the FOI Act with respect to domestic law enforcement agencies (see para 59(a) of our previous submission).

38. New section 122.4 is not subject to any amendments. It remains almost identical to section 70 of the Crimes Act, replicating the well-documented problems with that offence. We reiterate our view that is difficult to see the necessity of new section 122.4 in light of the other offences introduced by the Bill (see paras 48-50 of our previous submission).

3.2 The conduct criminalised in the Bill remains too broad

39. The proposed amendments do not address the excessive breadth of conduct captured by new sections 122.1-122.3, and replicate this breadth in the new proposed offence in new section 122.4A.

40. We refer the Committee to paras 62-65 of our previous submission, noting in particular that the ALRC firmly stated that conduct other than disclosure would not be appropriate in general provisions applying to all Commonwealth information.

3.3 Public interest disclosure remains insufficiently protected

41. The proposed amendments do not address the public interest disclosure defence, beyond the changes made to the defence available for journalists/those engaged in reporting news. We remain concerned that the drafting of Schedule 2 is not aligned to the *Public Interest Disclosure Act* (**PIDA**).

42. We reiterate the points previously made regarding the gaps between the proposed criminal offences and the scheme available under the PIDA:

    (a) The PIDA is only available for public officials. There is no mechanism to protect public interest disclosures from outsiders, who are captured in proposed new section 122.4A;

    (b) The defence in new section 122.5(4) only extends to "communication of information", and not to the other forms of conduct which may comprise an offence;

    (c) The PIDA has a broad carve out for "intelligence information".

43. We note that the PIDA does not contain a general public interest protection. Moreover, in his 2016 review of the PIDA, Mr Philip Moss AM described the scheme as "complex", concluding

that "by adopting legalistic approaches to decision-making, the PID Act's procedures undermine the pro-disclosure culture it seeks to create." We are therefore concerned that prior to addressing the inadequacies of the PIDA the government proposes to significantly expand secrecy offences.

3.4 The dramatic increase in penalties remains a serious concern

44. The proposed amendments do not address the penalties provided for by the Bill, except in creating a separate structure of penalties for "outsiders". The maximum penalties remain 15 years for offences under ss 122.1-122.2, or 20 years for an aggravated offence under s 122.3.

45. The new offences for outsiders in s 122.4A attract a maximum penalty of 10 years' imprisonment (or 3 for offences arising from conduct apart from the communication of information). This exceeds the current maximum of 7 years in current section 79 of the *Crimes Act*, which only applies to offences where the defendant intended to prejudice the security or defence of the Commonwealth. It also exceeds the ALRC's recommended maximum of 7 years for all secrecy offences.

46. As previously stated, any law that criminalises expression must grapple with the chilling effect that is created on *lawful* forms of expression, because of the possible threat of criminal sanction. This effect is worsened where the penalties are so severe. We reiterate the points made in paras 81-83 of our previous submission, and strongly recommend that the penalties in Schedule 2 be lowered to at least the level recommended by the ALRC.

4. Schedule 1 of the Bill

47. Our previous submission was limited to the concerns raised by Schedule 2 of the Bill, so as to allow us to engage with the issue of secrecy offences in depth. **However, we are concerned that the espionage offences proposed in Schedule 1 of the Bill also disproportionately burden freedom of expression.**

48. The proposed amendments would make some changes to Schedule 1. Those amendments address some of the problems of using security classification as an element of the Schedule 1 offences, and we welcome this. However, they do not address the broader concerns about the offences introduced and amended by Schedule 1, raised by the Law Council of Australia, Human Rights Watch, Australian Lawyers for Human Rights and others in submissions to this Committee.

49. The Bill would repeal existing espionage offences in s 91.1 of the *Criminal Code* and replace them with a number of offences classified into three groups: espionage offences, offences of espionage on behalf of a foreign principal, and espionage-related offences.

50. **Generally, we adopt the recommendations and findings of the Law Council of Australia**. In particular, we recommend that Division 91 be withdrawn and redrafted after consultation. However, here we draw attention to a number of key features, whose overlap contributes to the unjustified breadth of the espionage offences.

(a) "National security" is defined extraordinarily broadly and the proposed amendments do not engage with this issue. The definition, in new section 90.4, includes "political, military or economic relations" with another country or other countries. The expansion of the concept of national security to include economic relations is not justified and runs counter to the common understanding of the term. A potentially huge array of information might also concern Australia's political relations with other states. The breadth of this definition expands the breadth of conduct captured and criminalised by the relevant offences in Division 91. At the very least, paragraph (e) of s 90.4(1) must be removed.

(b) Many of the offences in Division 91 do not include harm as an element. For example, under s 91.1(1), a person may commit an offence punishable with life in prison, if they deal with information that **concerns** Australia's national security (broadly defined), where they intend that their conduct will prejudice Australia's national security *or advantage the national security of a foreign country*, and the information is made available to a foreign principal as a result. **There is no requirement that the dealing result in any harm to Australia's national security.** The HRLC adopts the Law Council's recommendation that the Bill be amended to introduce an express harm requirement, at a minimum for outsiders.

(c) A number of the offences rely on security classification. We refer to our comments above in paras 24-26, which apply equally in the context of Schedule 1.

(d) The breadth of the offences is extended by the many types of conduct which constitute "dealing" under s 90.1(1), as we identified in relation to the Schedule 2 offences, and the broad existing definition of "information" in s 90.1, which includes information, true or false, and opinions.

(e) The penalties provided for in Division 91 are among the most serious available, up to imprisonment for life. They should only be applied to carefully circumscribed offences that are of equivalent seriousness to the types of violent offences that attract such penalties elsewhere in Australian law.

(f) There are only limited defences available to offences in Division 91 that are insufficient to protect conduct that is in the public interest.

51. **The combination of these features means the espionage offences are far broader than necessary to protect national security information, and risk capturing a range of**

communications and conduct made or performed in good faith, in the regular course of journalism, business or academia (for example), that cause no harm to Australia. This is a clearly disproportionate imposition on freedom of expression.

52. The espionage offences are not the only offences in Schedule 1 to raise serious questions about their compatibility with human rights. In relation to the other offences in Schedule 1, we refer the Committee to the submissions of the Law Council of Australia, the Civil Liberties Councils, Human Rights Watch and Australian Lawyers for Human Rights.

Appendix

Recommendations of the Australian Law Reform Commission Report 112: Secrecy Laws and Open Government in Australia regarding the application of secrecy offences to non-Commonwealth officers

Recommendation 6-6

There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where:

(a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) in breach of the general secrecy offence; and

(b) B knows, or is reckless as to whether, the information has been disclosed in breach of the general secrecy offence; and

(c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in Recommendation 5–1.

Recommendation 6-7

There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where:

(a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) on terms requiring it to be held in confidence;

(b) B knows, or is reckless as to whether, the information has been disclosed on terms requiring it to be held in confidence; and

(c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in Recommendation 5–1.