Secrecy offences: the wrong approach to necessary reform

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

22 January 2018

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Contact

Dr Aruna Sathanapally (Director), **Hannah Ryan** (Lawyer), **Angela Chen** (Secondee Lawyer)

Human Rights Law Centre, Sydney

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/

Executive summary

The secrecy offences currently in the *Crimes Act 1914* are over-broad and overdue for reform. While the Bill takes the appropriate first step of repealing them, it provides for a new regime which replicates many of the offences' existing problems and dramatically increases the scope of the criminalisation of handling of Commonwealth information.

This submission sets out the six key concerns raised by the proposed secrecy offences, contained in Schedule 2 of the Bill. These are that:

- Criminal offences for the disclosure of information should only be introduced where the particular disclosure caused harm, or was intended to cause harm, to an essential public interest, such as the security and defence of Australia. This was central to the conclusions of the ALRC on the need to reform the law, and accords with Australia's obligations under international human rights law. However, the Bill does not consistently adopt a harm requirement before a person is convicted of a serious criminal offence. In fact, the Bill includes an offence (in new section 122.4) that is substantially similar to the outdated s 70 of the Crimes Act being replaced.
- Where the Bill does adopt a harm-based approach, it extends protection beyond essential public interests to other interests (such as information likely to "harm or prejudice relations between the Commonwealth and a State or Territory") which are appropriately protected by administrative and employment obligations, not serious criminal offences. This is again contrary to the ALRC's recommendations and Australia's international obligations.
- The proposed criminal offences extend to an excessive breadth of information (including information to which the public may have a right of access under freedom of information laws), types of conduct (including mere possession of information) and to all persons.
- The Bill does not sufficiently protect whistleblowers acting in the public interest, with the excessive breadth of the new offences creating several gaps between the protection available in the *Public Interest Disclosure Act 2013* and the defences included in Schedule 2.
- The Bill dramatically increases penalties from the current law, again contrary to the recommendations of the ALRC, to some of the most severe terms of imprisonment available under Australian law. This raises serious risk of a chilling effect that extends beyond the conduct covered by the offences to lawful communications about government. It would serve to intimidate public servants rather than encourage a culture of open government.
- The Bill's reliance on internal security classification of documents as the basis for general criminal offences is wholly inappropriate.

This type of legislation has no place in a healthy democracy, in which open government and the freedom to scrutinise government must be maintained, and those who expose wrongdoing must be supported and protected.

In our submissions, the secrecy offences proposed in the Bill are disproportionate to the objective of the legislation and need to be substantially redrafted to ensure that Australian law balances legitimate interests in protecting certain government information with the principles that are essential to the long term health of Australia's public institutions and democratic culture.

Recommendations:

1. **Schedule 2 be removed from this Bill and redrafted in line with the ALRC's recommendations.**
2. **Reform of Commonwealth secrecy offences extend to specific secrecy offences.**
3. **Reform of Commonwealth secrecy offences extend to strengthening the *Public Interest Disclosure Act 2013* and/or that new secrecy offences include a general public interest defence, to protect against the criminal conviction of whistleblowers.**

Contents

1. Introduction

1. The Human Rights Law Centre (**HRLC**) welcomes the opportunity to comment on the *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (**the Bill**), specifically, on its provisions relating to secrecy offences (contained in Schedule 2 of the Bill).

2. The HRLC has previously called for the amendment of the current secrecy offences in line with the recommendations made by the Australian Law Reform Commission's 2009 report, *Secrecy Laws and Open Government in Australia Report* (**ALRC Report**).[1] The report's recommendations have never been implemented. However, the ALRC Report remains a vital resource on the approach Australia should take to secrecy offences, supported by deep research and stakeholder consultation.

3. This submission sets out the core principles of Australian democracy that must guide the formulation of criminal offences for the disclosure and communication of information (Part 2) followed by an overview of the research and recommendations as to the best approach to protecting government information (Part 3), substantially drawing on the work of the ALRC. It then sets out six principal reasons why the proposed secrecy offences are dangerously overbroad and should not pass in their current form (Part 4). Our recommendations are contained in Part 5.

2. Open government and freedom of expression: core principles of Australian democracy

2.1 Healthy democracy relies on transparency in government

4. For decades, Australia has recognised the importance of open government, transparency and public accountability and enacted a series of reforms that have taken a modern approach to government information. Indeed, the existing secrecy offences in the *Crimes Act 1914* are a relic of the past, and their repeal is overdue.

5. The *Freedom of Information Act 1982* (**FOI Act**) created a positive right to access government information, subject only to exemptions where necessary for the protection of select public interests and to maintain personal privacy. The law was intended "to increase recognition that information held by the Government is to be managed for public purposes, and is a national

[1] HRLC, *Safeguarding Democracy*, February 2016, <http://static1.squarespace.com/static/580025f66b8f5b2dabbe4291/5812996f1dd4540186f54894/581299ee1dd4540186f55760/1477614062728/HRLC_Report_SafeguardingDemocracy_online.pdf?format=original>.

resource,"[2] and its objects are stated to be to promote Australia's representative democracy by contributing towards:

(a) increasing public participation in Government processes, with a view to promoting better informed decision making;

(b) increasing scrutiny, discussion, comment and review of the Government's activities.[3]

6. Justice McHugh, formerly of the High Court, has set out clearly the importance of taking a broad understanding of the information that Australians have a legitimate public interest in knowing:

> In the last decade of the twentieth century, the quality of life and the freedom of the ordinary individual in Australia are highly dependent on the exercise of functions and powers vested in public representatives and officials by a vast legal and bureaucratic apparatus funded by public moneys. How, when, why and where those functions and powers are or are not exercised are matters that are of real and legitimate interest to every member of the community. Information concerning the exercise of those functions and powers is of vital concern to the community. So is the performance of the public representatives and officials who are invested with them. **It follows in my opinion that the general public has a legitimate interest in receiving information concerning matters relevant to the exercise of public functions and powers vested in public representatives and officials. Moreover, a narrow view should not be taken of the matters about which the general public has an interest in receiving information**. With the increasing integration of the social, economic and political life of Australia, it is difficult to contend that the exercise or failure to exercise public functions or powers at any particular level of government or administration, or in any part of the country, is not of relevant interest to the public of Australia generally. **If this legitimate interest of the public is to be properly served, it must also follow that on occasions persons with special knowledge concerning the exercise of public functions or powers or the performance by public representatives or officials of their duties will have a corresponding duty or interest to communicate information concerning such functions, powers and performances to members of the general public**.[4]

7. Of course, we recognise that a functioning government relies on select information remaining confidential. The release of certain information known to government officials may jeopardise essential public interests but also the privacy of individuals who provide personal information to government. We further recognise that in designing a regime to govern the disclosure of government information, criminal offences for disclosure have a role to play where serious harm is caused, or is intended to be caused, by the person disclosing the information. However, this role is necessarily a **limited** one, given the availability of other, more appropriate methods of dealing with the disclosure of the majority of government information (set out below in Part 3).

8. Although it may be uncomfortable, whistleblowers are a necessarily important aspect to the integrity of the Commonwealth public service. Intimidating potential whistleblowers with onerous criminal penalties does a disservice to the public service. In the equivalent context of the United

[2] FOI Act, s 3(3).

[3] FOI Act, s 3(2).

[4] *Stephens v West Australian Newspapers Ltd* (1994) 182 CLR 211 at 264-265 (emphasis added).

Kingdom Civil Service, Sir Jeremy Heywood (Cabinet Secretary and Head of the Civil Service) has put the importance of whistleblowers in no uncertain terms, stating:

> Transparency means not being able to pick and choose what is visible to scrutiny, it should shine a light into every corner of public life and public service. We fatally compromise this principle if we allow uncomfortable truths to be hidden or covered up.
>
> Having proper and credible procedures in place to accommodate whistleblowers and their concerns, not only protects them but the integrity of public services. The system itself should facilitate not intimidate…**We want a culture that encourages people to raise concerns and to blow the whistle if they are not heard. We also want a culture that learns from concerns being raised and whistleblowing.** In such an environment, public services can only improve, the occasion for whistleblowing will decline, and the reputation of honest, conscientious public sector workers and civil servants - the vast majority - will be preserved.[5]

2.2 Freedom of expression

9. Secrecy offences engage freedom of expression by criminalising certain types of communication, but also more broadly, by deterring the free flow of information and public discussion about government. Criminal offences, and even more so those which carry substantial terms of imprisonment, create a powerful disincentive to engaging in expression that may, in fact, be lawful because of available defences or the manner in which the law is interpreted and applied.

10. Both under international law and under the Australian Constitution, freedom of expression about matters of government is a fundamental right. Under international law, the United Nations Human Rights Committee has observed that "in circumstances of public debate concerning public figures in the political domain and public institutions, the value placed by the [International Covenant on Civil and Political Rights] upon uninhibited expression is particularly high."[6] Under Australian law, the foundations of the constitutional implied freedom of political communication lie in the requirement that electors be able properly to choose their parliamentary representatives, which requires the free flow of information concerning government.

11. Freedom of expression under international law can be restricted in certain circumstances, where necessary "for the protection of national security or of public order, or of public health or morals".[7] "Public order" means "the sum of rules which ensure the functioning of society or the

[5] Sir Jeremy Heywood, 'Whistleblowers' on *Civil Service Blog*, 17 December 2014, <https://civilservice.blog.gov.uk/2014/12/17/whistleblowers/> (emphasis added).

[6] Human Rights Committee, *General Comment No 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [38].

[7] *International Covenant on Civil and Political Rights*, open for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976), art 19(3).

set of fundamental principles on which society is founded."[8] In order to be lawful, any limitation on freedom of expression must be proportionate to a legitimate objective.[9]

12. Under international law, open government is protected as a dimension of freedom of expression. Article 19(2) of the International Covenant on Civil and Political Rights (**ICCPR**) requires State parties to guarantee the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers. This paragraph "embraces a right of access to information held by public bodies."[10] States which withhold information must justify that as an exception to the right.[11]

13. Reporting to the United Nations General Assembly in 2015, the Special Rapporteur on the promotion and the protection of the right to freedom of opinion and expression said of the right of access to information:

> …to be necessary, a restriction must protect a specific legitimate interest from actual or threatened harm that would otherwise result. As a result, general or vague assertions that a restriction is necessary are inconsistent with article 19. However legitimate a particular interest may be in principle, the categories themselves are widely relied upon to shield information that the public has a right to know. **It is not legitimate to limit disclosure in order to protect against embarrassment or exposure of wrongdoing, or to conceal the functioning of an institution**.[12]

14. The Global Principles on National Security and the Right to Information (known as the Tshwane Principles), developed by 22 groups after consulting over 500 experts, give guidance on the obligations under Article 19 in the secrecy context. Relevantly, they provide that:

> **Principle 43: Public Interest Defence for Public Personnel**
>
> (a) Whenever public personnel may be subject to criminal or civil proceedings, or administrative sanctions, relating to their having made a disclosure of information not otherwise protected under these Principles, the law should provide a public interest defense if the public interest in disclosure of the information in question outweighs the public interest in non-disclosure.
>
> …
>
> **Principle 46: Limitations on Criminal Penalties for the Disclosure of Information by Public Personnel**
>
> (a) The public disclosure by public personnel of information … should not be subject to criminal penalties, although it may be subject to administrative sanctions, such as loss of security clearance or even job termination.

[8] UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 41st sess, E/CN.4/1985/4 (28 September 1984) [22].

[9] Ibid [10].

[10] Human Rights Committee, *General Comment No 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [18].

[11] David Kaye, Special Rapporteur, *Promotion and Protection of the Right to Freedom of Opinion and Expression*, 70th sess, UN Doc A/70/361 (8 September 2015) 5 [8].

[12] Ibid 5-6 [9] (emphasis added).

(b) If the law nevertheless imposes criminal penalties for the unauthorized disclosure of information to the public or to persons with the intent that the information will be made public the following conditions should apply:

(i) Criminal penalties should apply only to the disclosure of narrow categories of information that are clearly set forth in law;

Note: If national law provides for categories of information the disclosure of which could be subject to criminal penalties they should be similar to the following in terms of specificity and impact on national security: technological data about nuclear weapons; intelligence sources, codes and methods; diplomatic codes; identities of covert agents; and intellectual property in which the government has an ownership interest and knowledge of which could harm national security.

(ii) The disclosure should pose a real and identifiable risk of causing significant harm;

(iii) Any criminal penalty, as set forth in law and as applied, should be proportional to the harm caused; and

(iv) The person should be able to raise the public interest defence, as outlined in Principle 43.

Principle 47: Protection against Sanctions for the Possession and Dissemination of Classified Information by Persons Who Are Not Public Personnel

(a) A person who is not a public servant may not be sanctioned for the receipt, possession, or disclosure to the public of classified information.

(b) A person who is not a public servant may not be subject to charges for conspiracy or other crimes based on the fact of having sought and obtained the information.

Note: This Principle intends to prevent the criminal prosecution for the acquisition or reproduction of the information. However, this Principle is not intended to preclude the prosecution of a person for other crimes, such as burglary or blackmail, committed in the course of seeking or obtaining the information.

Note: Third party disclosures operate as an important corrective for pervasive over-classification.

15. Freedom of expression is also partially protected by Australian domestic law, most significantly through the constitutional implied freedom of political communication. Like international law, determining compatibility with the implied constitutional freedom involves a proportionality inquiry. A law that burdens the freedom must be "reasonably appropriate and adapted" to advance a legitimate object.[13] This proportionality test demands that the law be justified as suitable, necessary (without an obvious alternative means which would achieve the same objective in a less rights-restrictive way) and adequate in its balance.[14]

16. Secrecy offences have been found to engage the implied freedom.[15] The impugned regulation in *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, which provided that officials were not permitted to disclose "any information about public business or anything of which the employee has official knowledge", was found to

[13] *Lange v Australian Broadcasting Corporation* (1997) 189 520; *Coleman v Power* (2004) 220 CLR 1.

[14] See *McCloy v State of New South Wales* [2015] HCA 34 (7 October 2015) per French CJ, Kiefel Bell and Keane JJ at [2]-[5]. See also *Brown v Tasmania* [2017] HCA 43 (18 October 2017).

[15] See *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.

disproportionately burden the implied freedom of communication because of its catch-all nature: it did not differentiate between species of information or the consequences of disclosure.[16] In that case, Finn J commented:

> Official secrecy has a necessary and proper province in our system of government. A surfeit of secrecy does not…
>
> The dimensions of the control [the regulation] imposes impedes quite unreasonably the possible flow of information to the community—information which, without possibly prejudicing the interests of the Commonwealth, could only serve to enlarge the public's knowledge and understanding of the operation, practices and policies of executive government.[17]

17. In a recent review of the impact on journalists of the secrecy provision in s 35P of the *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**), the Independent National Security Legislation Monitor (**INSLM**) (the Hon. Roger Gyles AO QC) concluded that there were strong arguments that the provision was invalid due to the operation of the implied freedom of political communication. The INSLM identified three key flaws with the provision:

    (a) it lacked an express harm requirement for breach (of the basic offence);

    (b) recklessness was the fault element in relation to the consequences of disclosure (in the case of the aggravated offence);

    (c) it prohibited the disclosure of information already in the public domain.[18]

    He further identified the breadth of the information caught as weighing against its proportionality to the object of protecting national security.[19] He concluded that these factors combined to give substance to the argument that the provision was unconstitutionally disproportionate.

18. **Accordingly, the relevant inquiry in the context of secrecy laws is whether the restrictions on freedom of expression are necessary and proportionate for the protection of national security or public order (or a legitimate object of this order), in order to be constitutional and compatible with Australia's international obligations.**

[16] *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [101].

[17] Ibid [98]-[99].

[18] Independent National Security Legislation Monitor, *Report on the Impact on Journalists of Section 35P of the ASIO Act* (October 2015) 23.

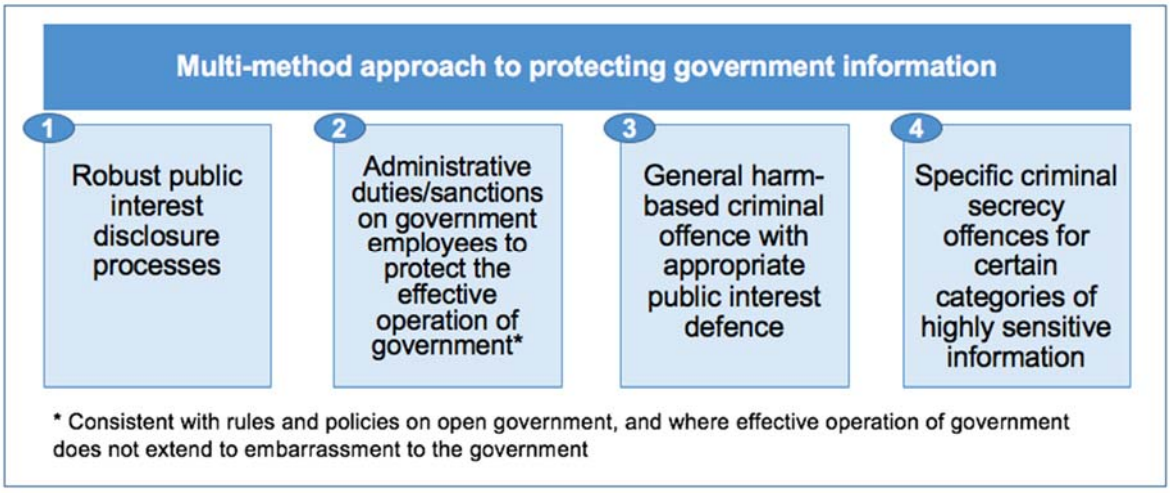
[19] Ibid 106.

3. A proportionate approach to protecting government information

3.1 A multi-method approach

19. The issue of the appropriate role of secrecy offences in the management of government information – including intelligence and national security information – has been the subject of sustained attention in Australia and in comparable countries in recent years. This work has established the need for a **multi-method approach** to protecting government information: there are several complementary tools available within which the use of criminal offences is reserved only for the most serious unauthorised disclosures of information. This was the position taken by the ALRC after considerable research and consultation.

20. Accordingly, in order to be a proportionate limitation on freedom of expression or freedom of political communication, the protection of government information ought to employ criminal offences only for disclosures that cause harm to essential public interests (such as prejudicing the protection of public safety, damaging the defence of the Commonwealth or endangering the life and physical safety of any person), not for the full range of unauthorised disclosures of government information, for which other tools are available and appropriate.



21. The *first element* of a proportionate approach is the existence of robust processes for lawful public interest disclosure by government employees and others who are in possession of government information. The best way to ensure a balance between government accountability and protecting information, the release of which would cause serious harm to a public interest, is to provide a sufficiently independent lawful release valve for information in the public interest, immune from sanctions. This reduces the need for a whistleblower to engage in unauthorised sharing of information to, for instance, expose malfeasance or dishonest information provided to the public by a politician. A complement to the internal avenue for public interest disclosure

is the ultimate power of a court to determine, in the event of external disclosure, whether the disclosure, on balance, was in the public interest. This safeguard, which may be very rarely engaged, is necessary in the event that internal processes are ineffective, delayed or compromised. It is especially vital where a person is facing criminal conviction, rather than, say disciplinary action or the loss of employment.

22. The introduction of the *Public Interest Disclosure Act 2013* (**PIDA**) was a welcome step in Australia, however Australian law falls below what is sufficient to secure effective public interest disclosure. In particular, the PIDA falls short of providing a general public interest protection, placing a series of definitional and procedural criteria in place before the court can examine whether the disclosure is not, on balance, contrary to the public interest in the event of external disclosure.[20] The complexity of this regime compromises the practical protection offered to a potential whistleblower in possession of important information. Additionally, the PIDA includes a broad carve out for "intelligence information" whether or not the disclosure of that information would cause harm to the security and defence of Australia, or an interest of equivalent seriousness. **Any legislation seeking to broaden and increase criminal sanctions for whistleblowers (as the Bill does) makes the existing weaknesses in the PIDA more dangerous.**

23. The *second element* of a proportionate approach is the use of administrative or civil sanctions in relation to government employees. **There are a wide range of disciplinary or employment based sanctions that may be applied to those who engage in unauthorised disclosure of information that is likely to prejudice the effective operation of government and is not in the public interest.**

24. The ALRC reached the conclusion that prejudice to the effective operation of government, for the purpose of administrative obligations, should be prejudice arising either from the nature of the information (i.e. information that would not be subject to release to the public under the FOI Act or otherwise), or where an employee did not take reasonable steps to comply with the agency's information handling policy. It ought not be sufficient that the disclosure could result in embarrassment to the government to establish prejudice.[21]

25. The *third element* is a general secrecy offence that criminalises disclosure that causes serious harm to an essential public interest. That is, that the specific disclosure of information by a government employee did, or was reasonably likely to, or was intended to, for example, damage the security or defence of the Commonwealth, or endanger the life or physical safety of any person.

[20] See *Public Interest Disclosure Act 2013* (Cth), Part 2 Division 2.

[21] ALRC Report, Recommendation 12-2.

26. **The need for the general criminal offence to be harm-based in this manner was central to the ALRC conclusions and recommendations as to what ought to replace the current secrecy offences (further explained in 3.2 below)**.

27. The *fourth element* of a proportionate approach is specific secrecy offences where necessary and proportionate to the protection of essential public interests of sufficient importance to justify criminal sanctions, and which differ in significant and justifiable ways from general secrecy offences.[22]

28. The Bill deals only with general secrecy offences, leaving untouched the vast number of specific secrecy offences found in Commonwealth law. In 2009, the ALRC Report identified **506 secrecy provisions in 176 pieces of legislation**, with many of the provisions creating criminal offences for breaches. Since that time, further specific secrecy offences have been enacted, for instance, within the *Australian Border Force Act 2015,* which have themselves raised serious concerns regarding the protection of whistleblowers and severe limits on freedom of expression.[23]

29. The ALRC set out a series of careful recommendations for the amendment or repeal of this vast number of specific secrecy offences under Australian law (including the need for a harm-based approach, as explained below). **This process is long overdue, and the repeal of ss 70 and 79 of the *Crimes Act 1914* is a missed opportunity to address the full extent of the problem of outdated and excessive secrecy offences under Australian law**.

3.2 A harm-based approach to secrecy offences

30. The best way to ensure that only those disclosures that *must* be prevented in the public interest are criminalised is to incorporate a serious harm requirement as an element of the offence. That is, the criminalisation of the disclosure of information will only be necessary where that particular disclosure has caused harm, was likely to cause harm or was intended to cause harm, to an essential public interest.

31. This approach accords with Australia's obligations under international law. The United Nations Human Rights Committee has stated that:

> Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security…are crafted and applied in a manner that conforms to the strict requirements of [Article 19(3)]. **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.[24]

[22] See ALRC Report Recommendations 8-1 – 8-3.

[23] Parliamentary Joint Committee on Human Rights, Report 11 of 2017, 72-83.

[24] Human Rights Committee, *General Comment No 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [30] (emphasis added).

32. The Committee has further explained that:

> When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in **specific and individualised** 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**.[25]

and observed in relation to the United Kingdom's *Official Secrets Act* that:

> The state party must ensure that its powers to protect information genuinely related to matters of national security are **narrowly utilized and limited to instances where the release of such information would be harmful to national security**."[26]

33. These statements strongly support the requirement for harm to an essential public interest, such as national security, being an element of any general secrecy offence. A criminal conviction for the disclosure of information which did not, or was not reasonably likely to or intended to, result in harm is highly unlikely to meet the demands of the proportionality test in the individual case, thereby violating the ICCPR (Article 19).

34. A harm-based approach was central to the ALRC's recommendations. The ALRC stated:

> The ALRC's key recommendation for reform in the criminal context is that, in most cases, the prosecution should be required to prove that a particular disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm to specified public interests, such as the security or defence of the Commonwealth. **In the absence of any likely, intended or actual harm to an essential public interest, the ALRC has formed the view that the unauthorised disclosure of Commonwealth information is more appropriately dealt with by the imposition of administrative penalties or the pursuit of contractual remedies**.[27]

35. The ALRC explained that this approach struck the appropriate balance between two competing public interests:

> This approach balances the need to protect certain Commonwealth information with the public interest in an open and accountable system of government. It also means that the sanctions of the criminal law are reserved for the more serious cases of unauthorised disclosure.[28]

[25] Ibid, [35] (emphasis added).

[26] Human Rights Committee, *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant: Concluding Observations - United Kingdom of Great Britain and Northern Ireland*, 93rd sess, UN Doc CCPR/GBR/CO/6 (30 July 2008) [24] (emphasis added).

[27] ALRC Report, 99-100 [4.2] (emphasis added).

[28] ALRC Report, 138 [4.157].

4. Key concerns raised by Schedule 2 of the Bill

36. The Bill's secrecy provisions are contained in Schedule 2.

37. Schedule 2 repeals ss 70 and 79 of the *Crimes Act 1914*. In their place, it introduces a modified version of s 70, which criminalises disclosures of Commonwealth information by Commonwealth officers (new section 122.4). In place of s 79, which criminalises the disclosure of official secrets, it creates two new offences relating to "inherently harmful information" and information that would "cause harm to Australia's interests" (new sections 122.1 and 122.2). Additionally, the Bill creates an aggravated form of the latter two offences (new section 122.3).

38. We welcome the repeal of the *Crimes Act* offences, which are outdated and overdue for reform. There are further positive dimensions to the proposed reform, such as the introduction of harm-based offences in new section 122.2 and the introduction of defences in new section 122.5.

39. **However, the overall regime in Schedule 2 replicates many of the existing problems with the current law, while dramatically increasing the criminal penalties and the scope of available offences, for the handling of government information. The result is a proposal that takes a disproportionate approach to protecting government information by relying too heavily on excessive criminal offences and heavy terms of imprisonment, where other tools are reasonably available and appropriate.**

40. This submission does not address the full detail of each of the provisions in Schedule 2. Rather, we set out in this section the six key concerns, in view of the requirements under both international law and Australian constitutional law to take a proportionate approach, and the elements of a proportionate approach set out above. We consider that these concerns, taken together, are best addressed by the removal of Schedule 2 to allow for substantial redrafting, rather than specific amendments to the proposed framework of offences.

41. Nor does this submission address the provisions in the other Schedules to the Bill. With respect to the espionage offences in the Bill, we refer the Committee to the serious concerns raised by Human Rights Watch in its submission. We further note the importance of maintaining a consistency in public interest protections across secrecy and espionage offences, so that the weakness of safeguards in one regime does not compromise the other by allowing for an alternative avenue for the prosecution of disclosure in the public interest.

4.1 The Bill does not adopt a consistent harm-based approach

42. The general secrecy offences created in new sections 122.1 and 122.4 impose criminal liability without a requirement that the disclosure (or other kind of handling of information) caused, were likely to cause, or were intended to cause, any harm.[29]

43. **New section 122.1** adopts an approach that criminalises disclosure based on broad categories of information. These categories are set out under the proposed new definition of "*inherently harmful information*". The information that would fall within each category is to include information of any kind, whether true or false and whether in a material form or not, and including an opinion or a report of a conversation.[30]

44. New section 122.1 does not include any requirement that the person handling the information in any of a wide range of ways intends to cause harm, is likely to cause harm, or in fact causes harm to an essential public interest. Nor does new section 122.1 require that the person know that the information falls within any of the specified categories, and where the relevant category is security classified information, the Bill imposes strict liability.

45. The category of security classified information raises distinct concerns which are set out in full below (see 4.6).

46. Other categories are also likely to include both information that would damage essential public interests and information that would not cause such harm. As the Explanatory Memorandum acknowledges, the category of "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" covers a wide range of information. It may include the type of information which is provided to Commonwealth agencies or regulators, such as the Therapeutic Goods Administration in relation to the approval of new medicines, or to the Australian Competition and Consumer Commission, the Australian Securities and Investment Commission, or any number of regulators whose work would only occasionally relate to national security, defence, or public interests of that order. It is acknowledged that the unauthorised disclosure of information provided to Commonwealth authorities, in certain circumstances, could prejudice the effective operation of government, or personal privacy. However, as set out above, other tools are readily available to deal with that policy problem. The criminal law is neither necessary nor proportionate.

[29] The one exception, applying to new section 122.1, is sub-paragraph (b) of the definition of "inherently harmful information", which in its terms includes a requirement that communication of the information would, or could reasonably be expected to damage the security or defence of Australia.

[30] Adopting s 90.1 of the *Criminal Code*, see Sch 2 new section 121.1.

47. New section 122.1 would also protect against disclosure of information of a foreign law enforcement agency or a foreign intelligence agency (without limiting the scope to Australia's allies) and it is far from clear that such disclosures would inherently damage Australia's interests so as to remove the need for such damage to be an element of the criminal offence.

48. **New section 122.4** introduces a provision which is substantially similar to s 70 of the *Crimes Act 1914*, wasting a valuable opportunity to address longstanding, principled critiques of the section. Like s 70, new section 122.4 would penalise unauthorised disclosures by former and current Commonwealth officers of information they were under a duty not to disclose. Indeed, the only material difference between s 70 and new section 122.4 appears to be that new section 122.4 specifies that the duty not to disclose the information must arise "under a law of the Commonwealth".[31]

49. New section 122.4 thereby replicates the recognised flaws in s 70 of the *Crimes Act 1914,* not only in lacking any requirement that the disclosure result in harm, but the further two serious problems identified by the ALRC:

    (a) Both s 70 and new section 122.4 apply to *any* information a Commonwealth officer learns in their job regardless of its nature or sensitivity (provided they have a duty not to disclose it).[32] The ALRC concluded that "it is not appropriate to impose criminal sanctions for breach of any duty not to disclose Commonwealth information."[33]

    (b) Like s 70, new section 122.4 applies where a person had a "duty not to disclose" the relevant information,[34] but does not provide that duty itself, or even the Acts in which those duties are contained. Instead, the duty must be found elsewhere. While it is an improvement to specify that the duty must be under a law of the Commonwealth, this does not solve the essential difficulty of uncertainty facing a person potentially subject to this criminal offence.[35]

50. Ultimately, it is difficult to see the necessity of new section 122.4 in light of the other offences introduced by the Bill, which cover a wide array of conduct. It is hard to imagine conduct which would offend this section, but not fall foul of new sections 122.1 or 122.2, and that would merit criminal sanction rather than administrative penalties.

[31] New section 122.4(1)(d).

[32] ALRC Report 89 [3.100].

[33] Ibid 123 [4.101].

[34] New section 122.4(1)(c).

[35] See ALRC Report, 119-123.

4.2 The Bill extends to harm to interests which do not merit use of serious criminal offences

51. By contrast, the offences in **new section 122.2** do incorporate a harm requirement, requiring the relevant conduct in each new offence causes harm, or will or is likely to cause harm to "Australia's interests". However, the interests included within the definition of "cause harm to Australia's interests" (set out in new section 121.1) include both essential public interests and public interests of a lower order, that do not warrant the application of criminal sanctions.

52. The ALRC provided, in its first recommendation for what should follow the repeal of ss 70 and 79 of the *Crimes Act 1914*, that the only essential public interests justifying the creation of criminal offences (as distinct from administrative sanctions) were:

(a) damage to the security, defence or international relations of the Commonwealth;

(b) prejudice to the prevention, detection, investigation, prosecution or punishment of criminal offences;

(c) danger to the life or physical safety of any person; or

(d) prejudice to the protection of public safety.[36]

53. The interests identified by the ALRC, in our view, are more appropriately captured within the legitimate objectives of national security and public order, so as to be capable of justifying a limitation on freedom of expression under international law.

54. While recognising the importance of the protection of government information the disclosure of which would harm the effective operation of government, the ALRC recommended that administrative obligations (attracting sanctions such as suspension or termination of employment) were the appropriate method to use where necessary.

55. However, the offences in new section 122.2 would extend to information that is likely to "harm or prejudice relations between the Commonwealth and a State or Territory" or harm *or prejudice* Australia's international relations in *any* way (see new section 121.1). New section 122.2 therefore criminalises, with very severe penalties, information that could clearly be a matter of considerable, legitimate public interest, and it is easy to imagine that it would include information that the principles of open government – and the constitutional protection for political communication – would require be freely shared and communicated.

56. Moreover, new section 122.2 would extend to information that threatened not only criminal but also civil penalty proceedings, contrary to the ALRC's view that it would be excessive to impose criminal sanctions in general secrecy offences for information that threatened civil proceedings.[37]

[36] ALRC Report, Recommendation 5-1.

[37] ALRC Report, 155-167 [5.55].

57. It should be noted that the ALRC reached its recommendations on the interests that were appropriate to protect through administrative sanctions and the interests that merited the use of the criminal offences with the benefit of a broad-based consultation and an advisory committee that was comprised of a wide range of senior public servants. It should be understood that its suggestions are neither radical nor impractical. However, instead of adopting the ALRC's recommendations, the Bill takes the approach of broadening the use of criminal sanctions to address a range of interests beyond essential public interests as identified by the ALRC, raising serious concerns, in particular for Commonwealth employees who may face not only serious workplace consequences for a wide range of conduct, but also imprisonment for up to 15 to 20 years, for handling or sharing information (including the expression of opinions).

4.3 The Bill's provisions are excessively broad in terms of information, conduct and persons captured

58. Overall, Schedule 2 is drafted in terms which are too broad to be a proportionate limitation on freedom of expression, given that it criminalises the possession and sharing of information and communication on matters relating to government. As referred to above, the scope of information covered is very broad, and this is further compounded by the breadth of conduct and persons captured by the proposed offences in new sections 122.1,122.2 and 122.3. The overall effect is a set of offences that have no place in a healthy democracy.

Breadth of information

59. As noted in some examples above, the breadth of the provisions is such that they will criminalise the disclosure of information to which Australians have a right of access under the FOI Act.[38] For example:

a) New section 122.1 criminalises disclosure of "information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency," whereas the FOI Act only exempts documents whose disclosure would or could reasonably be expected to "disclose lawful methods or procedures for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law the disclosure of which would, or would be reasonably likely to, prejudice the effectiveness of those methods or procedures" or "prejudice the maintenance or enforcement of lawful methods for the protection of public safety".[39] The secrecy offence also extends to foreign law enforcement agencies, whereas the FOI Act exemption does not.

[38] The right of access is prescribed in *Freedom of Information Act 1982* (Cth), s 11.

[39] FOI Act, s 37(2)(b) and (c).

b) New section 122.2 extends to information the handling of which would harm or prejudice relations between the Commonwealth and a State or Territory, whereas under the FOI Act, a document the disclosure of which would, or could reasonably be expected to, cause damage to relations between the Commonwealth and a State is only *conditionally exempt* from release, meaning that it is only exempt if its release would, on balance, be contrary to the public interest (see ss 11A and 47B of the FOI Act). New section 122.2 contains no such public interest test.[40]

c) The FOI Act provides no exemption for security classified information (the difficulties of security classification are explained below, in 4.6). Rather than merely relying on security classifications or other protective markings, the FOI decision-maker has to independently turn their mind to the question of whether a document's disclosure would cause damage to specified public interests. As such, persons disclosing security classified or marked "for Australian Eyes Only" information could be caught under the proposed offences, notwithstanding that the information could be legally obtained under the FOI Act.

60. A public servant should not be open to criminal conviction for releasing information which a member of the public could successfully request under the FOI Act. For the law to be otherwise would be unprincipled and incoherent. Indeed, it should be the case that secrecy offences criminalise only the most serious subset of that information which the public is not readily entitled to access.

Breadth of persons

61. The offences in new sections 122.1-122.3 are not limited in their application to current and former Commonwealth officers but can apply to *any* person. These new offences apply equally to Commonwealth officers and outsiders, without any additional circumstances needing to be present. Outsiders should not be subject to the same offences and penalties as government insiders, given the distinct duties owed by Commonwealth officers. This accords with the view of the ALRC, the Gibbs Committee review of Commonwealth criminal law, and, in the *ASIO Act* context, the INSLM.[41]

[40] FOI Act, ss 11A and 47B

[41] See ALRC Report, Recommendations 6-6 and 6-7; H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991) 323; Independent National Security Legislation Monitor, *Report on the Impact on Journalists of Section 35P of the ASIO Act* (October 2015), available at: https://www.inslm.gov.au/sites/default/files/files/impact-s35p-journalists.pdf, 22-23.

Breadth of conduct

62. The conduct captured by new sections 122.1-122.3 extends beyond disclosure of information to five types of conduct, which taken together, would capture conduct from mere possession of information through to publishing information to the public.[42]

63. The breadth of the conduct regulated is entirely inappropriate for general criminal offences across all types of information in an enormous range of contexts. As firmly stated by the ALRC, introducing offences covering conduct other than disclosure would "not be appropriate in general provisions applying to all Commonwealth information".[43] Other conduct is better dealt with through administrative procedures.[44]

EXAMPLE

The risks of the breadth of the proposed laws can be demonstrated by a hypothetical example.

A person, Evelyn, who is an outsider to government (not an intelligence agent or even a Commonwealth employee or contractor) may have a friend who works at the Office of National Assessments. The friend tells Evelyn about their parental leave policy, and Evelyn takes a note of it. Evelyn has now "dealt" with that information by making a record of it, and the information, being a policy made by a domestic intelligence agency, appears to fall within the definition of "inherently harmful information". Despite owing no duty arising from employment or any other duty, Evelyn may have violated new section 122.1(2), which is a criminal offence carrying a 5 year maximum term. This is the same maximum penalty that applies under the *Commonwealth Criminal Code* to a Commonwealth public official who abuses public office (s 142.2 of the *Criminal Code*).

64. The cumulative effect of the breadth of information, conduct and persons captured is extraordinary. For this reason alone, it is very difficult to see how these proposed laws could be sufficiently targeted as to be compatible with Australia's international obligations, and Schedule 2 raises potential issues of constitutionality.

65. In addition to the concerns raised above in relation to the three key offence provisions (new sections 122.1, 122.2 and 122.4), this is a further reason why, in our view, Schedule 2 needs to be substantially redrafted to capture conduct that is of sufficient gravity to be criminalised.

4.4 The Bill does not sufficiently protect public interest disclosure

66. It should be recognised that by introducing the defence provision in new section 122.5, the proposed legislation is an improvement on the existing state of the *Crimes Act* offences.

[42] See in particular, the expansive definition of 'deal with' in new section 121.1(1), referring to new section 90.1(1) of the *Criminal Code*.

[43] ALRC Report 203 [6.80].

[44] ALRC Report 204 [6.83].

Moreover, the effect of the PIDA is to immunise a person who makes a "public interest disclosure" within the terms of that Act from criminal liability for making the disclosure (which is reflected in new section 122.5(4)).

67. **However, the sheer breadth of the offences created in new sections 122.1-122.4 creates significant risks that the defences in new section 122.5, including the protections of the PIDA, do not sufficiently protect the public interest.**

68. The guiding principle is to be that criminal prosecution and conviction ought not extend to disclosures which are, properly, on balance, in the public interest (even if serious employment or other consequences may be imposed). Criminal secrecy offences for government information must only capture conduct that is on balance, harmful to an essential public interest. Narrowly targeted offences and robust immunities for public interest disclosure are preferable to achieve this, but a general public interest defence may also serve as fallback protection.

69. While a public interest disclosure scheme should be, ideally, the principal avenue for public interest disclosures, there may be occasions that fall outside the scheme available, or where the scheme fails to operate as it should. This is why it is important to ensure alignment between the scheme in the PIDA and the reform of general secrecy offences, including ensuring that a court is the ultimate arbiter of whether an immunity ought to apply in the event of an external disclosure.

70. The proposed regime in Schedule 2 would appear to create several gaps between the protection available in the PIDA and the defence available in **new section 122.5(4**). First, the mechanism under the PIDA is only available for public officials, defined to extend to a range of Commonwealth employees and officials and those performing a Commonwealth contract. However, the offences in new sections 122.1-122.3 extend beyond those public officials to any person, creating a gap between the two regimes, and criminalising the disclosure of information by persons who do not have access to the PIDA. The most obvious and logical way to address this gap would be to limit the offences to the same set of public officials, and put in place separate subsequent disclosure offences that are more appropriately targeted and/or have appropriate defences in place.

71. Second, the PIDA has a broad carve out for "intelligence information", which extends to, among other things, all information that has originated with, or has been received from, an intelligence agency, including any summary or extract of such information[45], without any requirement that disclosure of the specific information would cause or is likely to cause harm. This means that there is no lawful avenue for disclosure of any such information in the public interest. This makes it dangerous to legislate for serious criminal offences that apply to such

[45] *Public Interest Disclosure Act 2013*, s 41.

information that do not include a public interest defence, or are not, at the very least, limited to disclosure that harms an essential public interest.

72. Third, while the proposed offences would extend to a broad range of conduct beyond disclosure, the defence in new section 122.5(4) extends only to "communication of information". The PIDA itself does not cover the range of conduct that is proposed to be included in the offences. This leaves persons acting in the public interest open to prosecution for a broad set of offences that are covered neither by the immunity in s 10 of the PIDA or any public interest defence.

73. It is difficult to assess how the proposed regime or the PIDA could be amended to address these difficulties. In short, the excessive nature of the offences places the regime out of step with the PIDA. This is a further reason why we have reached the view that Schedule 2 needs to be substantially redrafted.

74. While the proposed public interest defence specifically for journalists in **new section 122.5(6)** is welcome, this alone is not sufficient to ensure freedom of expression, or even a free press, if protections are not extended to journalists' sources.

75. Additionally, the defence includes a requirement that a journalist has engaged in "fair and accurate reporting" *in addition to* having dealt with or held the information in the public interest. This requirement appears duplicative, as well as difficult to apply, particularly for a jury. The requirement of "fair and accurate" reporting as a defence appears to have been drawn from the defamation and contempt contexts, however there the defence relates to the report of particular proceedings (such as court proceedings or parliamentary proceedings) where a record allows later assessment of fairness and accuracy. This is different from a general assessment of what is "fair and accurate" for any type of communication a journalist may engage in. That assessment will be rendered more difficult in light of the possible contentious nature of any subject a journalist may report on using information falling within the terms of new sections 122.1-122.5. Our view is that this defence would be improved by the removal of the requirement in 122.5(6)(b).

4.5 The dramatic increase in penalties would generate a chilling effect across a wide range of matters of public interest

76. The current offences in ss 70 and 79 of the *Crimes Act 1914* carry a maximum term of imprisonment of 2 years, with the exception of certain official secrets offences involving an intention of prejudicing the security or defence of the Commonwealth, in which case it is 7 years.

77. The Bill proposes penalties of up to 15 years imprisonment within new sections 122.1 and 122.2, with the aggravated offence in new section 122.3 attracting a maximum penalty of 20 years, which is an order of magnitude greater than the current offence in s 70. There is no evidence of a pressing need for such a dramatic increase in the available terms of imprisonment, to the very gravest criminal sentences provided for under Australian law. For context, elsewhere in the

Criminal Code, the penalty of 20 years imprisonment is imposed for the offence of subjecting a person to cruel, inhuman and degrading treatment or certain war crimes.

78. Several of the aggravating circumstances that would attract the highest penalties are themselves troubling, for instance, that the person held any security clearance (even at the lowest levels) with no need for their security clearance to be connected in any way to the offence; or that the offence involved 5 or more records (which given the broad definition of record in the Commonwealth *Criminal Code*, may be very easily satisfied).

79. Moreover, the extreme nature of the penalties provided for in new sections 122.1-122.3 can be seen in comparison with the penalty for the new section 122.4 offence, which is a maximum of 2 years imprisonment.

80. The ALRC recommended penalties no higher than the existing law, that is, 7 years.[46] This too was in the context of a far more limited general criminal offence and the use of administrative duties to capture much of conduct and information contained in Schedule 2.

81. Elsewhere in this submission we have queried the necessity for criminal penalties for the captured conduct, where administrative penalties may be available in many cases. The concept of a "chilling effect" refers to the inhibition or discouragement of the legitimate exercise of one's rights because of the possible threat of legal sanction. Where criminal offences are included in the law, and even more so when they are accompanied by the types of terms of imprisonment set for the most heinous violent crimes, they cast a shadow beyond the conduct actually captured by the offence.

82. If Schedule 2 is passed, a person who handles or discloses information in relation to the Commonwealth government faces the prospect of severe penalties. Even if defences are available, or the information may not be captured, they necessarily face the uncertainty of how the law would apply to them, and whether arrest and prosecution may proceed. The regime in Schedule 2 is focused exclusively on deterring the disclosure of government information. It is not in keeping with the values of open government, and encouraging Commonwealth employees to understand government information as ordinarily public information, except in select circumstances.

83. Moreover, as stated above in paragraph 8 even the most senior public servants believe that a system of good government "should facilitate not intimidate" whistleblowers in the public interest. There will always be pressures on those in possession of information not to speak out, such as the personal or professional cost. This Bill, with its broad reach, and onerous penalties, would severely compromise that goal.

[46] ALRC Report, Recommendations 7-4 and 7-5.

4.6 The Bill's reliance on security classification by government departments is wholly inappropriate for a general criminal offence

84. Under the proposed law, any document with a security classification will be defined as "inherently harmful", and its disclosure is accordingly criminalised by new section 122.1. The accompanying fault element for an offence involving the disclosure of security classified information is strict liability: so a person may be convicted even if they did not know or were not reckless as to security classification (new section 122.1(5)). Classification and other protective markings also constitute some of the aggravating circumstances in new section 122.3.

85. There is no mechanism by which the security classification by the particular agency is confirmed as being correct prior to the commencement of proceedings, nor is there an available defence under the proposed law that the security classification was incorrect.[47]

86. Protective markings, such as security classifications, have a clear administrative role to play in the Commonwealth public service. However, they are wholly inappropriate for inclusion in the creation of a general criminal offence, without any scope for the court or jury to revisit whether the security classification was correctly applied, for the following reasons:

(a) The system of protective markings and the security classification system is not based in legislation. Instead, it is guided by the "Information security management guidelines - Australian Government security classification system" [48] (the **Guidelines**) published by the Attorney General's Department. The Guidelines do not accurately reflect how protective markings are applied in practice; they are supplemented and may in some instances be overridden by policies developed by each governmental agency (which are not publicly available).

(b) There is no requirement for reviewing or reconfirming initial protective markings and security classifications. The Guidelines merely suggest confirmation of initial markings where the protective marking is not normal or standard for that agency.[49] The Guidelines defer to agencies to create their own policies in relation to their personnel applying and

[47] New section 121.3 provides that the Attorney-General may certify that information has had, or had at a specified time, a security classification or a specified level of security classification. In criminal proceedings under Division 122, that certificate will constitute prima facie evidence of the matters certified in it. However, the provision does not require the Attorney-General to certify that any classification was correctly used. This is therefore no safeguard against incorrect classification.

[48] The Attorney-General's Department, *Information security management guidelines - Australian Government security classification system*, version 2.2, approved November 2014 and amended April 2015. See also <https://www.protectivesecurity.gov.au/Pages/default.aspx>.

[49] The Attorney-General's Department, *Information security management guidelines - Australian Government security classification system*, version 2.2, approved November 2014 and amended April 2015, [31].

reviewing protective markings. As such, criminal liability could turn on the decision of a single government agency official, regardless of seniority.

(c) There is a known and documented practice of over-classification. The Australian National Audit Office found in their 1999 report "Operation of the Classification System for Protecting Sensitive Information" that all audited agencies incorrectly classified files, with over-classification being the most common occurrence.[50] The Australian Government has not imposed or suggested agencies impose repercussions on individuals for over-classification in the Guidelines, its Protective Security Policy Framework or legislation.

(d) There is no mandatory system to ensure timely declassification of information with the exception of archiving Commonwealth records approximately 21-30 years in accordance with regime in the *Archives Act 1983* (Cth).[51]

87. Until November 2017, the use of security classification as a basis for criminal liability was unprecedented. The *Australian Border Force Act 2015* (Cth) (**ABFA**) as amended in November 2017 is the only legislation where this approach has been adopted. The Senate Standing Committee for the Scrutiny of Bills[52] and the Parliamentary Joint Committee on Human Rights[53] both raised concerns with the amendments to those secrecy provisions, notwithstanding greater protection afforded under the ABFA in relation to confirmation of security classifications prior to commencement of proceedings (which is absent in Schedule 2).[54]

88. The proposed amendments present a clear rule of law issue. Even where classifications are correct, criminal liability would be triggered by virtue of the protective marking itself rather than the substance of the underlying information. Put another way, when applying a protective marking, the government agency personnel is also determining whether future disclosure of the document would trigger criminal liability. Yet this process is not governed by law.

89. As set out above at paragraph 59, under the FOI Act security classification or other protective markings are not a determinative indicator of whether a document is one to which the public have a right of access.[55] It follows that it is wholly inappropriate for these markings to determine criminal liability, or aggravated criminal liability.

---

[50] Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information, Audit Report* 7 (1999) [2.84].

[51] *Archives Act 1983* (Cth), s 3(7).

[52] Senate Standing Committee for the Scrutiny of Bills, Scrutiny digest, op. cit., 1–3.

[53] Parliamentary Joint Committee on Human Rights, Report 11 of 2017, [2.73].

[54] *Australia Border Force Act 2015* (Cth), s 50A.

[55] The Guidelines emphasise that the "presence or absence of a protective marking will not affect a document's status" under the *Freedom of Information Act 1982* (Cth): *Information security management guidelines - Australian Government security classification system,* [14].

5. Recommendations

90. For the reasons set out above, **we recommend that Schedule 2 be removed from this Bill**, so that it can be substantially redrafted into a form that is consistent with fundamental tenets of Australia's system of government, being freedom of political communication and open government. We do not consider that the concerns raised above can be properly addressed through piecemeal amendment of the proposed scheme, which, as it stands, has no place in Australia's democracy.

91. In making this recommendation we note that the inclusion of secrecy offences within this particular Bill is questionable in any event, given the Bill's focus on espionage and foreign interference. The offences in Schedule 2 do not engage these issues.

92. Nor has any case been made for urgency at this time for the Crimes Act 1914 offences to be repealed and replaced, in particular given the lack of any urgency since the ALRC Report in 2009. Given that the reforms do not follow the blueprint provided by the ALRC's research and consultation, and would impact the entirety of the Commonwealth public service and its contractors, as well as the information available to the Australian public, it is essential that they are carefully considered, with the benefit of a full pre-legislative consultation.

93. We further recommend that the reform of Commonwealth secrecy offences extend to specific secrecy offences, in line with the ALRC's recommendations, and that it extend to either strengthening the Public Interest Disclosure Act 2013 and/or to the creation of a general public interest defence, to protect against the criminal conviction of whistleblowers.