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

***A joint submission from**:*
NSW Council for Civil Liberties
Liberty Victoria
Queensland Council for Civil Liberties
South Australian Council for Civil Liberties
Australian Council for Civil Liberties

14/2/2018

1 Preliminary Comments

The councils for civil liberties across Australia (New South Wales Council for Civil Liberties, Liberty Victoria, Queensland Council for Civil Liberties, South Australia Council for Civil Liberties and the Australian Council for Civil Liberties) are grateful for the opportunity to make this submission to the inquiry by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into *the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017.* (The Bill)[1]

This Bill is part of a major package of proposed legislation relating to national security and foreign intervention. Apart from the very large and very significant Bill under consideration in this inquiry, two other closely related bills are simultaneously before the PJCIS for review: *the Foreign Influence Transparency Scheme Bill 2017* and the *Security of Critical Infrastructure Bill 2017*[2]. The important and linked *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill* 2017 is simultaneously before the Joint Standing Committee on Electoral Matters.

When introducing this Bill into the Parliament, the Prime Minister emphasised both the collective importance and the interlocked nature of these bills: '*Together, they add up to the most important overhaul of our counterintelligence legislative framework since the 1970s'.*[3]

The CCLs agree. We are therefore seriously concerned that the timing and the time frame available for the public consideration of these lengthy and technically complex bills and for the production of submissions to the PJCIS and to the Parliamentary Joint Standing Committee on Electoral Matters Committee (PJSCEM) were inadequate[4]. This is notwithstanding the welcome extension of time for submissions to the 14th February. It was not possible, despite our very keen interest, for the joint CCLs to finalise responses on all these bills. We suspect this may have been the case with other volunteer civil society organisations with an interest and expertise in these areas.

[1] This submission has been updated since publication on the PJCIS site to insert 2 missed recommendations (nos 17 & 18) into the Summary of Recommendations on p56 and to change 'national infrastructure' to 'Public infrastructure' p46.

[2] There is also a less significant consequential bill – the Home Affairs and Integrity Agencies Legislation Amendment Bill 2017 before the PJCIS under the same timeframe. It is of relevance to the national security and foreign intervention bills given the pivotal role the Home Affairs portfolio will have in relation to national security and counter-terrorism.

[3] PM Second reading Speech Hansard 7/12/17.

[4] The bills were introduced into Parliament in the second week of December. The PJCIS inquiries were announced in mid-December and submissions were due on 22/1/18. A similar time frame applied for Electoral Funding and Disclosure Reform Bill. The Xmas and NY holidays meant most organizations were non-functional until the second week of January or later. On the 1st December the PJCIS extended the deadline for submissions on this Bill and the Foreign Influence Transparency Scheme Bill 2017 to 15th February 2018.

This submission from the CCLs does not cover all the important offences that are proposed in the Bill. We have given our fullest focus in the time available to the secrecy offences in schedule 2.

2 Stop Press- Secrecy of Information Offences

Since this submission was written the Government has indicated that it will be redrafting the secrecy offences to strengthen the available defence for journalists and their support staff, narrow the definitions of '*conduct that could cause harm to Australia's interests'* and *'inherently harmful information'* and ensure that outsiders (non-commonwealth officers) are only prosecuted for serious and dangerous conduct. [5]

While we will have await the amendment to the Bill to assess these promised changes, it appears they will address some of the most dangerous and unwarranted aspects of the proposed secrecy offences. Hopefully the reworking of key definitions will address some aspects of the lack of clarity that is such a problem in the Bill.

This move by the Attorney-General is in the right direction and is welcomed. However, the problems with the secrecy offences go beyond the issues identified by the Attorney-General.

It seems clear that the changes will not include a 'carve out' for journalists. Strong defences are better than weak ones- but uncertainty as to whether or not one will face prosecution will remain a major inhibitor for journalists and others wanting to disclose information in the public interest.

None of the changes appear to provide protections for whistle-blowers or others (academics, policy analysists, civil liberties and human rights advocates, health professionals etc.) who want to disclose information in the public interest. They do not address the unjustified huge increases in penalties.

There is a real question as to whether three general secrecy offences are necessary. As currently drafted there is considerable duplication and overlap.

There are also significant issues relating to the offences in schedule 1 of the Bill.

3 The Context

The Prime minister's statements in relation to this package of national security and foreign intervention legislation suggest that we face unprecedented threats on these fronts. He references

[5] *Federal War on news, truth*: The Saturday Paper 10-16 February 2018.

a recent report by ASIO initiated through the Prime Minister's Department which 'made significant investigative breakthroughs and delivered a series of very grave warnings'[6]. This report is classified.

The CCLs accept that foreign influence and interference is a significant and growing issue globally and for Australia. However, had it been possible for the public to have some explanation of the general nature of these 'grave warnings' possibly in a redacted version, it may have given some tangible substance to the description of the threat level as 'unprecedented'.

There are some high profile overseas examples of apparent successful foreign intervention in the democratic and electoral processes. The 2016 United States Presidential election drew international attention to the issue of foreign state interference in democratic and electoral processes, and is now under investigation by US Congress and the Federal Bureau of Investigation.

Russian intervention in elections has drawn the attention of the international press, although no formal findings have yet been made by either investigation. Foreign, particularly Russian, interference in civil process is also being investigated in relation to the 2016 United Kingdom vote on British departure from the EU (Brexit), as well as the 2017 French Presidential elections .

Foreign interference in democratic and electoral processes is a serious issue that threatens some of the most precious civil liberties: the right to vote and to representational democracy. The CCLs accept that Australia will not be an exception from this experience and that we need appropriate protective laws.

However, legislative response must be proportional to the nature of the threat, and it is not clear from the Bill, its explanatory memorandum or the second reading speeches what increased threats of foreign interference have been raised in relation to Australian elections and democratic processes that might explain the introduction of much broader offences which, in many instances, carry increased and very serious penalties.

We also consider that it is important that when framing laws to protect national security the Parliament ensures that fundamental liberties and rights and core democratic principles of Australian society are appropriately protected.
As a matter of generality, the CCLs will support measures that:

- are necessary;
- do not disproportionately undermine human rights and civil liberties;

[6] PM second reading speech Hansard 7/12/17.

- respect and uphold the rule of law;
- provide adequate protections from and constraints upon inappropriate executive power;
- maintain appropriate government accountability and minimise blanket secrecy provisions
- Protect legitimate whistle-blowers

4 Main Provisions of the Bill

In Schedule 1 the Bill proposes major changes and additions to current offences dealing with threats to national security, particularly those posed by foreign principals. In Schedule 2 the Bill proposes major changes to the current general secrecy laws which have long been subject to criticism and are overdue for reform.

This is a large Bill of major significance. The proposesd new or amended offences cover:

- amendments to espionage offences
- new foreign interference offences
- new and stronger secrecy offences
- new sabotage offences
- amendments to modernise treason and related offences
- new theft of trade secrets offence
- new aggravated offence for providing false and misleading information in the context of security clearance processes[7]

The Bill includes numbers of significant new, and sometimes interlocking, definitions, which are crucial to an understanding of the offences. In most cases they are expansive and sometimes loose definitions which individually and cumulatively extend the scope of many of the offences well beyond current legislation. In some of the offences the problem is lack of definition of key elements so that the meaning and scope of what is intended in the proposed legislation cannot be determined.

These proposed new and extended offences cover critically important areas of national security and the balance between open government and secrecy in democratic Australia.

[7] National Security Legislation Amendment (Espionage And Foreign Interference) Bill 2017 .Explanatory Memorandum (EFI Bill 2017 EM) p2.

5 CCLs' Position

There are aspects of the Bill we can support as appropriate modernising of existing offences. But there are many aspects which we see as unjustified overreach and the overall implications of this Bill, were it to be implemented in its current form, would be extremely damaging to many core aspects of Australia's democracy and open society.

The CCLs do not support the Bill in it is current form.

6 General Comment

Within the Bill, the new and expanded secrecy offences in Schedule 2 are of the greatest concern to the CCLs.

Schedule 2 creates a number of staggered new secrecy offences replacing the general secrecy offences in ss 70 and 79 of the Crimes Act *1914* (Cth) (Crimes Act**).**

These proposed secrecy offences, as drafted, are of great concern to the CCLs. They are unwarrantedly and dangerously expansive, excessively punitive and lack necessary clarity. They diverge without explanation from key recommendations of considered reviews of the current offences. They expand, without explanation the application of 9 of these offences to outsiders (persons other than commonwealth officers or entrusted persons currently covered) but ignore advice to create separate offences for insiders and outsiders.

These offences, because of their extraordinary reach and severity, will further undermine journalist's capacity to report on government activity, whistle-blowers willingness to disclose wrongdoing and incompetence in the public interest and will greatly restrict the free flow of information and Australians' right to freedom of expression on political and governmental matters.

In so doing, they constitute a further major step away from open government in Australia – which, in the view of the CCLs, is a grave miscall for the health of our democracy.

This is not a new concern. The CCLs have previously expressed concerns about the unhealthy proliferation of unwarranted secrecy offences at the Commonwealth level – most recently in

relation to the ASIO special intelligence operations secrecy offence and Australian Border Force legislation both of which we opposed. [8]

Because of their extraordinary reach, these new offences will have a more pervasive chilling effect than both of those offences.

Free speech, the free press, and the free flow of information are essential to democracy and should not be lightly curtailed. Australians enjoy a right to freedom of expression, particularly in relation to political and governmental matters. This is recognised at common law,[9] in the Constitution, and in international human rights instruments.[10]

The free press plays a crucial watchdog role in a democracy, supplying the public with information to guard against abuses of power and government's mistakes. To operate in this way, the free press depends on access to information and sources, including whistle-blowers within government and government agencies. Legitimate whistleblowers are essential to a healthy democracy for the exposure corruption and misuse of power to public scrutiny. Restricting whistleblowing reduces government accountability

The High Court has described the free flow of information from sources to journalists as 'a vital ingredient in the investigative journalism which is such an important feature of our society'.[11] More recently, the importance of investigative journalism and journalists' access to sources has been recognized by the Commonwealth and several state governments in their enactment of 'shield laws'.[12]

The offences introduced by this Bill will have, and appear intended to have, a major deterrent effect on legitimate whistleblowers, on the freedom of the media to report on abuses of power by government - even when these pose no harm or threat to Australia's interests or national security.

[8] Submission by the Joint CCLs: INSLM Review Impact on Journalists 22/4/15; and Submission by Joint CCLs to ALRC Inquiry on Traditional Rights and Freedoms 18/10/15.

[9] *Evans v NSW* [2008] FCAFC 130 (15 July 2008), [74], citing William Blackstone, *Commentaries on the Laws of England* (T. Tegg, 17th ed, 1830), Book 4, 151-152; TRS Allan, 'The Common Law as Constitution: Fundamental Rights and First Principles' in Cheryl Saunders (ed), *Courts of Final Jurisdiction: The Mason Court in Australia* (Federation Press, 1996) 146, 148, quoted with approval in *Minister for Immigration & Citizenship v Haneef* (2007) 163 FCR 414.

[10] For example, the right to freedom of expression contained in Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR).

[11] *John Fairfax & Sons Ltd v Cojuangco* (1988) 165 CLR 346, 356. See also *Liu v The Age Co Ltd* [2012]] NSWSC 12 (11 February 2012), [15], [162] - [164].

[12] *Evidence Act 1995* (Cth), Protection of journalists' sources s126H.

7 Current offences and proposals for reform

The Schedule 2 offences replace the current general secrecy offences in s 70 and s79 of the Crimes Act.

Disclosure of information by commonwealth officers

Section 70 of the Crimes Act provides that a current or past Commonwealth officer who publishes or communicates any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer, and which is his or her duty not to disclose commits an offence punishable by two years imprisonment.

Official secrets

Section 79 of the Crimes Act relates to unlawful communication of official secrets by Commonwealth officers. There are graduated offences by commonwealth officers : communication of the information with 'the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions' (7 years imprisonment); communication without the intention of prejudicing the security or defence of the Commonwealth (2 years imprisonment) and retaining information, refusing to comply with a lawful direction as to retention or disposal or failure to take reasonable care of information (6 months imprisonment).[13]

There are two offences relating to the unlawful receipt of secret information by a person with penalties 7 years or 2 years imprisonment. [14]

Reform of these offences has been repeatedly recommended over a long period – including from major reviews conducted by the Biggs Committee[15] in the early 1990s and, more recently, by the Australian Law Reform Commission (ALRC) Report on Secrecy Laws and Open Government in 2009[16]. The major and extensively researched ALRC report provided a broad and principled framework for reform as well as detailed recommendations on a new general secrecy offence. This report remains relevant and its recommendations for reform of these offences are considered and sensible.

The 2016 report by the Independent National Security Legislation Monitor, in response to widespread concerns about a specific secrecy offence in the ASIO Act, reviewed the history of

[13] Crimes Act Section 79(1), 79(2), 79(3),79(4)
[14] Ibid 79(5), 79(6).
[15] H Gibbs, R Watson and A Menzies, Review of Commonwealth Criminal Law: Final Report (1991).
[16] (ALRC Secrecy Report 2009). The ALRC report builds on the work of the Biggs Committee.

Commonwealth secrecy offences and made a number of observations and recommendations which also have particular relevance to these proposed offences.[17]

Some of the ALRC recommendations have been acted upon and the Explanatory Memorandum indicates where proposals are consistent with the ALRC recommendations. However, key ALRC recommendations for reform are not reflected in the proposed secrecy offences

Most critically, the proposed offences are not consistent with the key recommendation for 'repeal of the wide catch-all provisions' in the current offences and their replacement with a general secrecy offence based on the core principle that criminal sanctions should 'be reserved for behaviour that harms, is reasonably likely to harm or intended to harm essential public interests'. [18] As drafted the proposed secrecy offences go in the opposite direction.

The proposed offences also ignore the recommendation of the ALRC and the INSLM[19] that separate offences should be created for third party subsequent disclosures even though all but one of the offences apply to outsiders.

Many of the major problems with this Bill would have been avoided had the approach of the ALRC for the reform of the current general secrecy provisions been more fully incorporated.

8 Secrecy Offences s122 - Detailed Comment

The new general secrecy offences in section 122 are in four categories:

- 122.1 Inherently harmful information
- 122.2 Conduct causing harm to Australia's interests
- 122.3 Aggravated offences
- 122.4 Unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers.

There are 10 new offences across these categories. All except 122.4 are applicable to both commonwealth officers and other persons.[20]

The Bill incorporates a suite of defences for the offences in this section. While the CCLs do not think these are adequate, their inclusion is consistent with the recommendations of the ALRC and

[17] Independent National Security Legislation Monitor: Report on the impact on journalists of section 35P of the ASIO Act 2016 (INSLM Report S35P 2016).
[18] (ALRC Secrecy Report 2009)
[19] INSLM Report S35P 2016) P3 and (ALRC Secrecy Report 2009) Recommendation 6-7
[20] (EFI Bill 2017.EM) p240.

remedies a weakness in the current general secrecy offences. [21]

9 Inherently harmful information s122.1

There are 4 offences in the category of 'inherently harmful information':

i) Communication of inherently harmful information-penalty 15 years imprisonment

ii) Dealing with inherently harmful information – penalty 5 years imprisonment

iii) Information removed from, or held outside, proper place of custody- penalty 5 years

iv) Failure to comply with direction regarding information - penalty 5 years imprisonment.

Communication of inherently harmful information 122.1(1)

The most serious offence is the '*communication of inherently harmful information'* 122.1(1).

There are three problems with this offence: the absence of a harm requirement, the overly expansive definition of harmful information categories and the unexplained and unwarranted (more than) doubling of the current penalties for s79 offences.

122.1(1) A person commits an offence if:

(a) the person communicates information; and

(b) the information is inherently harmful information; and

(c) the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.[22]

Strict liability applies to (1)(b). The communication of any information within the general category is a criminal offence with a maximum penalty of 15 years imprisonment.

Harm element

No harm element is included as the information communicated is defined as 'inherently harmful'. This is a contentious approach as it is clear that '*while a category may be directed to protecting a legitimate public interest, the disclosure of information within that category will not always cause,*

[21] (EFI Bill 2017)s122.5
[22] (EFI Bill 2017) s 122.1(2)

or be likely to cause, harm'.[23] From this perspective it follows that generally the offence should require a harm element to distinguish between a harmful and unharmful disclosure.

The ALRC was strong in its support for the harm element being expressly included in the general secrecy offence, but accepted that there were some contexts in which unlawful disclosure of categories of information could be criminalised without the harm element. This was if '*the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit or the harm is to the relationship of trust between individuals and the Australian Government integral to the regulatory functions of government'*[24]**.**

The ALRC recommended this approach should only apply for specific secrecy offences drafted in a specific agency context**.**

The ALRC accepted that intelligence agency's information- and that of a small number of other agencies such as the ATO- could be justifiably accepted as inherently harmful[25]. The CCLs accept that there are some tightly defined categories of information which could justify an inherently harmful categorisation. We do not accept that this should encompass blanket coverage of intelligence agencies' information.

More importantly, we do not accept that offences relating to 'inherently harmful information' do not require an express harm element- particularly in relation to outsiders.

In terms of consistency, we note that the information relating to an ASIO 'special *intelligence operation'* would certainly fit any definition of 'inherently harmful information'. S35P which criminalises the disclosure of this information is a specific secrecy offence drafted to fit the specific agency function. In its initial legislated form, the offence included a harm element in the aggravated offence. Following the INSLM's recommendations, this offence was amended in 2016 to include separate offences for insiders and outsiders. Both the basic and the aggravated offences for outsiders included a harm element.

The CCLs consider that this offence should be redrafted to include a harm element and to remove the strict liability requirement in relation to 1(b) "*the information is inherently harmful information'*.

[23] ALRC Secrecy Report 2009) p288
[24] ALRC Secrecy Report 2009) recommendation 8.2 This recommendation was in relation to specific secrecy offences.
[25] ALRC Secrecy Report 2009) See discussion in chapter 8

10 Definition - *Inherently harmful information'* 122.1(1)

The scope of information captured by this offence is determined by the list of 'categories of information' deemed to be 'inherently harmful information'. They are:

(a) security classified information;

(b) information the communication of which would, or could reasonably be expected to, damage the security or defence of Australia;

(c) information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions;

(d) 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;

(e) Information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency.[26]

Some of these categories have a tenuous connection to Australia's essential interests and some are so expansive they are likely to include much information which would be of trivial significance and unlikely to cause other than trivial harm to Australia's essential public interests.

(a) '**Security classified information'**

It is not clear what will be captured by this category. For the purposes of this Bill it means 'information that has a security classification' which is itself defined as : '*has the meaning prescribed by the regulations'.*[27]

No guidelines are included to give clarity or certainty as to what kind/level of classified information is appropriate to include in the regulations. It is therefore not possible know what could be encompassed within 'security classified information' for the purpose of this offence from the specifications within the Bill. This is not appropriate.

Apart from this omission, there are questions as to whether 'security classified information' is an appropriate and sufficiently robust category for this serious offence.

[26] EFI Bill 122.1(1)
[27] EFI Bill 90.5

The classification system is based on guidelines issued by the Attorney General's Department, and not on legislation. [28]. There is no requirement to review initial classification, and there is a documented practice of over-classification. There are no repercussions for over-classification in the guidelines or legislation. There is also no mandatory system of de-classification[29]. Security classifications are at different levels from low to very high.

This definition gives no clarity as to what level of security or kind of information could be included. It may include very low level 'security classified information' which if unlawfully communicated, would cause no harm to Australia's interests.

Furthermore, classified information that is likely to be harmful to Australia's national interests will be captured by the other information categories.

The ALRC noted the problems and decided:

> *Therefore, the ALRC is not recommending the enactment of specific secrecy offences that cover 'national security classified information', preferring instead an approach that recognises that particular government agencies that obtain and generate sensitive information of this kind may need an agency-specific secrecy offence*[30]

The CCLs recommend that paragraph (a) 'security *classified information'* should be removed from the list of 'inherently harmful information' categories.

(b) **'Information which would, or could reasonably be expected to, damages the security or defence of Australia'**

This is an appropriate category and is consistent with the ALRC's recommendations on the general secrecy offences.[31] It relates directly to national security and defence and includes a harm element.

(c) **'Information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions'**

This very wide category is only somewhat narrowed by the specification that the information was made 'in connection with the agency's functions.

[28] Australian Government Attorney-General's Department, Australian Government Protective Security Manual (PSM) (2005).
[29] See discussion ALRC Secrecy Report 2009 p 285ff.
[30] (ALRC Secrecy Report 2009) p288
[31] (ALRC Secrecy Report 2009): Recommendation 5-1.

However the inclusion of foreign intelligence agencies –neutral, friendly and unfriendly alike– does not seem justified. It is not clear that disclosure of all or most information from foreign intelligence agencies would pose a significant threat to Australia's security or national interests.

Such a provision would inhibit journalists, academics, consultants and others from public reporting on, or discussion of activities of foreign intelligence agencies which may be highly relevant to the public interest.

The Explanatory Memorandum offers no explanation for the inclusion of foreign agencies. It's comment on the category (c) is:

> *'The compromise of information made or obtained by the intelligence services could reasonably be expected to cause serious damage to Australia's national security. Even small amounts of such information could, when taken together with other information, compromise national security, regardless of the apparent sensitivity of the particular information—this is*
> *referred to as the 'mosaic approach' to intelligence collection.'* [32]

The CCLs recommend that paragraph (c) be narrowed in its scope by the removal of the reference to '*a foreign intelligence agency*.'

> ***'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 covers all commonwealth agencies or authorities and seems to cover all information that a person may be required to provide to any of them. Again this will capture information that should not be deemed 'inherently harmful'. This should be more tightly drafted and limited to agencies\authorities requiring information that is likely to be harmful to Australia's essential interests.

The CCLs recommend that paragraph (d) should be redrafted to narrow the agencies or contexts in which the information is likely to be harmful to Australia's essential interests.

> '***Information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency'***

This category is appropriate in that it would capture much sensitive, inherently harmful information whose unlawful communication would cause harm to law enforcement agencies operations and capacities and Australia's essential interests.

[32] (EFI Bill 2017:EM) p231

But it will also capture much information that will have no significant bearing upon the effective operation of law enforcement agencies and is not likely to harm Australia's essential interests.

It also appears to significantly duplicate paragraph (b) in that the '*security or defence of Australia'* is defined as including "the operations, capabilities or technologies of, or methods

The Explanatory Memorandum states that the definition of inherently harmful information "*is comprised of five categories of information the unauthorised disclosure of which would, or would be reasonably likely to, harm essential public interests".*[33]

This is clearly not accurate. These broad categories of information will encompass considerable amounts of information which will not harm Australia's essential interests. The scope of the information categories should therefore be narrowed as recommended.

Notwithstanding this, the express incorporation of a harm element is the only effective protection against criminalising disclosure of information that does not threaten harm to Australia's essential interests.

Penalty

The 15 years imprisonment maximum penalty imposed for this offence is greater than the penalty for the most serious of the current official secrets offences[34] - which is 7 years imprisonment with intention to cause harm, or 2 years imprisonment without intention to cause harm.

The ALRC recommended the maximum penalty for the general secrecy offence should be 7 years imprisonment.[35]

There is no persuasive argument presented for the more than doubling of the current maximum penalty for this offence. The Explanatory Memorandum only states the penalty must be 'adequate to deter and punish' a worst case offence:

> *'The commission of this offence would have serious consequences for the security and defence of Australia, or for the flow of information to the Commonwealth in connection with essential public functions. The maximum penalty needs to be adequate to deter and punish a worst case offence, including intentional or corrupt disclosures of inherently harmful*

[33] (EFI Bill 2017 EM) p237
[34] Crimes Act 1914 s79
[35] [35] (ALRC Secrecy Report 2009): Recommendations 7-4, 7-5

information, and disclosures that may irreparably damage the defence or security of Australia for decades.'[36]

This is not an explanation for the increase in the penalty. It provides no evidence - and the CCLs know of none - that would indicate that the current penalties are inadequate.

(We note that the INSLM did not query the maximum 10 years imprisonment penalty for the aggravated S35P secrecy offence. The CCLs considered the 10 year penalty in that context was severe. We maintain this view.)

Presumably the ALRC was also concerned with adequate punishment and deterrence for a worst case offence. The CCLs are not aware of evidence that indicates that 15 years imprisonment would be a greater deterrent than 7 years.

It will however certainly inhibit journalists and legitimate whistle-blowers. The CCLs do not support the substantial increase in the maximum penalty for this offence.

Redundant offence

The proposed CCL recommendations would improve this offence by limiting it to more appropriate categories of information, requiring an express harm element for the offence and reducing the penalty to a proportionate level.

However, the underlying problem is that this kind of offence is not appropriate to a general secrecy offence. The ALRC recommendation that these 'inherently harmful information' categories should be confined to specific secrecy offences which are agency specific.

The CCLs oppose its current drafting as a general secrecy offence.

Furthermore – as discussed at a later section – the broad information areas covered by this proposed offence are largely incorporated in the other two secrecy offences: communication causing harm to Australia's interests (122.2) and unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers (122.4).

The CCLs consider this offence to be redundant and recommend its removal from the Bill.

[36] (E&FI Bill 2017.EM) p242

Recommendation 1

The CCLs consider that the communication of inherently harmful information offence 122.1(1) is not appropriate for a general secrecy offence and is redundant within this Bill as its categories of 'inherently harmful information' substantially duplicate information covered by other proposed offences at 122.2 and 122.4.

The CCLs recommend it be removed from the Bill.

Failing this:

Recommendation 2

The CCLs recommend:

(i) that the communication of inherently harmful information offence (122.1(1)) be redrafted to include a harm element and to remove the strict liability requirement in relation to 1(b) "*the information is inherently harmful information'*.

(ii) The related offences 122.1(2), 122.1(3), 122.1(4), should be similarly redrafted to align with these changes

(iii) that the definition of 'inherently harmful information' at 122.1 be amended as follows:

- that paragraph (a) 'security *classified information'* should be removed from the list of 'inherently harmful information' categories.

- that paragraph (c) 'Information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions' be narrowed in its scope by the removal of the reference to 'a foreign intelligence agency.'

- that paragraph (d) ***'****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****'*** should be redrafted to narrow the agencies or contexts in which the information is likely to be harmful to Australia's essential interests

- that consideration be given to whether paragraph (e) is a redundant category given it is defined as a sub-category of 'security or defence of Australia' at paragraph(b).

(iv) that the maximum penalty for 'the communication of inherently harmful information' offence (s122.1(1)) should be reduced to a maximum of 7 years imprisonment to align with those in the current general secrecy offences and with the penalties proposed by the ALRC. The penalties for the related offences 122.1(2), 122.1(3), 122.1(4) should be similarly aligned.

11 Conduct causing harm to Australia's interests s122.2

Section 122.2 proposes a set of graduated information offences that involve 'conduct causing harm to Australia's interests':

i. communication causing harm to Australia's interests – penalty 15 years imprisonment
ii. (dealing with information causing harm to Australia's interests - penalty 5 years imprisonment
iii. removing or holding information causing harm to Australia's interests penalty 5 years imprisonment
iv. failure to comply with a direction regarding information - causing harm to Australia's interests- penalty 5 years imprisonment.

Communication causing harm to Australia's interests 122.2(1)

The basic offence in this category occurs when a person communicates information which either 'causes harm to Australia's interests' or 'will, or is likely to do so' - and 'the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity'.

The penalty is 15 years imprisonment.

Although it diverges in some aspects, this offence is clearly modelled on the general secrecy offence recommended by the ALRC.

Definition - cau*se harm to Australia's interests'* 121.1(1)

The scope of the information captured in this offence is determined by the definition of 'ca*use harm to Australia's interests'* at s121.1(1):

(a) interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of:

(i) a criminal offence against; or

(ii) a contravention of a provision, that is subject to a civil penalty, of: a law of the Commonwealth; or

(b) interfere with or prejudice the performance of functions of the Australian Federal Police under:

(i) paragraph 8(1)(be) of the Australian Federal Police Act 1979 (protective and custodial functions); or

(ii) the Proceeds of Crime Act 2002; or

(c) harm or prejudice Australia's international relations in relation to information that was communicated in confidence:

(i) by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and

(ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; or

(d) harm or prejudice Australia's international relations in any other way; or

(e) harm or prejudice relations between the Commonwealth and a State or Territory; or

(f) harm or prejudice the health or safety of the public or a section of the public.[37]

The ALRC recommended that the general secrecy offence should apply only to disclosure of Commonwealth information '*that did or was reasonably likely to, or intended t*o:

a. damage the security, defence or international relations of the Commonwealth;

b. prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;

c. endanger the life or physical safety of any person; or

d. prejudice the protection of public safety'[38]

[37] (EFI Act 2017) 121.1(1)

[38] ALRC Secrecy Report 2009): Recommendation 5-1.

The ALRC areas recommended by the ALRC for inclusion in the general secrecy offence are ones which are central to Australia's national security and essential national interests. The scope is appropriate and proportionate for a serious criminal offence.

However the areas the proposed offence will encompass in the proposed offence are considerably more expansive than these and will involve areas that are not central to Australia's national security or essential interests. The CCLs consider it necessary for these expansions to be clearly justified.

The Explanatory Memorandum says that (a), (c), (d) and (f) 'correspond with the categories of harm recommended by the ALRC. [39] This is the case, but it would be more precise to say they incorporate an expanded description of these areas.

The proposed offence also incorporates additional areas without explanation.

(a)(ii) '*a contravention of a provision, that is subject to a civil penalty, of a law of the Commonwealth.'*

The ALRC expressly excluded civil matters from its general secrecy offence as not likely to encompass matters posing a significant threat to Australia's national security of essential interests.[40] The CCLs agree that this is not an appropriate category.

This paragraph should be removed as a category from the definition of cause harm to Australia's interests.

(e) '*relations between the Commonwealth and a State or Territory'*.

While clearly important, commonwealth state relations are not central to – and certainly not confined to – matters of Australia's security or national interests.

The Gibbs Committee was of the view that: *'The relations between an Australian State and the Commonwealth Government are on a totally different plane from the relations between Australia and a foreign country.'*[41]

Also this is an area in which there is likely to be highly contestable, legitimate views as to what constitutes harm or benefit to relations between the Commonwealth and states particularly given many aspects of the relationship are driven by domestic politics.

[39] (EFI Act 2017 EM) p222.
[40] ALRC Secrecy Report 2009)
[41] Quoted in (ALRC report 2009) p168.

Relations between the commonwealth and a State or Territory should be removed should be removed as a category.

(c) harm or prejudice Australia's international relations in relation to information that was communicated in confidence

This additional reference to confidential information is a specific expansion of the general reference to 'international relations' in the areas recommended by the ALRC and is in addition to the proposed reference (d) in this offence which specifies 'international relations in any other way'.

There have been differing views as to whether this category of confidential information should be included in the general secrecy offence. The Gibbs Committee argued it should be, but the ALRC came to the conclusion it should not.

The ALRC came to this conclusion because not every confidential document passed from foreign governments and authorities or international organisations to Australia would damage international relations if disclosed and because of its basic position that categories of information were not appropriate for inclusion in the general secrecy offence.

> *…..the general secrecy offence should not include protected categories of information, such as information communicated in confidence. While the ALRC acknowledges that information damaging to relations between the Commonwealth and the states and territories requires protection, unauthorised disclosure of this kind of information should be addressed through intergovernmental arrangements, the imposition of administrative sanctions, or the pursuit of general law remedies. Where such information is sensitive for other reasons—for example, because it relates to national security, the enforcement of the criminal law, or public safety—unauthorised disclosures may be caught by other elements of the general secrecy offence.*[42]

While noting the difference of expert opinions, the CCLs do not support the specific inclusion of 'information communicated in confidence'' as an additional category of information the disclosure of which would harm Australia's international relations.

[42] (ALRC Report 2009) p168.

If the disclosure of confidential information is, or is likely to be, harmful to Australia's international relations, it will be captured by the general provision in (d)- with the removal of the last four words ('*in any other way'*).

Interfere with 121.1(1)(a) and (b)

At the more detailed level, the inclusion of 'interfere with' as an alternative to 'prejudice' in relation to (a) and (b) is not appropriate. 'Interfere with' does not necessarily imply damage or negative outcomes. It might result in enhancements. It does suggest a minor or intervention with a minor impact. ' Interfere' should be removed from the definition of cause of harm to Australia's interest at 121.1(1)(a) and (b).

We have elsewhere[43] noted that the definition of 'prejudice 'provided by the Explanatory Memorandum' needed to be redrafted to require more than 'trivial harm'. That applies in this context also.

Recommendation 3

The CCLs recommend that:

(i) the definition of '*cause harm to Australia's interests'* ss121.1(1) is amended to limit its scope to areas of significance to Australia's national security and essential interests by the removal of:

- (a)(ii) '*a contravention of a provision, that is subject to a civil penalty, of a law of the* Commonwealth and
- (e) 'relations between the Commonwealth and a State or Territory' and
- *(*c) harm *or prejudice Australia's international relations in relation to information that was communicated in confidence: i)by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and(ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; and*
- *the words "in any other way' from 121.1 (1)(d)*

- the words 'interfere with' from the definition of '*cause harm to Australia's interests* in 121.1(1)(a) and 121.1(1)(b)

[43] pp46-7 this submission.

ii. penalties for the offences in s122.3 be aligned with the ALRC recommendations on penalties for Commonwealth secrecy offences which have as a maximum 7 years imprisonment.

iii. the 'cause harm to Australia's interests offence ' 122.3 not be supported without these amendments.

12 Aggravated offence 122.3

The Bill includes an aggravated offence for each of the offences in sections 122.1 and 122.2. The aggravating factors to the underlying offences are:

(a) the person commits an offence against section 122.1 or 122.2 (the underlying offence); and

(b) any of the following circumstances exist in relation to the commission of the underlying offence:

(i) the information in relation to which the underlying offence is committed (the relevant information) has a security classification of secret or above;

(ii) if the commission of the underlying offence involves a record containing the relevant information—the record is marked with a code word, "for Australian eyes only" or as prescribed by the regulations for the purposes of this subparagraph;

(iii) the commission of the underlying offence involves 5 or more records each of which has a security classification;

(iv) the commission of the underlying offence involves the person altering a record to remove or conceal its security classification;

(v) at the time the person committed the underlying offence, the person held an Australian Government security clearance.

The penalty adds 5 years to the penalty for the underlying offence: so the penalties for the aggravated offence are 20 years imprisonment (rather than 15) and 10 years imprisonment (rather than 5). These are severe penalties well in excess of the penalties recommended by the ALRC.

The Explanatory Memorandum offers the following explanation:

> *The higher maximum penalty reflects the higher level of culpability associated with proof of the circumstances set out in paragraph 122.3(1)(b) and the extreme risk posed to Australia's national security in such cases. The penalties for the aggravated offence are consistent with the established principle of Commonwealth criminal law policy as set out in the Guide to Framing Commonwealth Offences to impose a higher penalty where the consequences of the offence are particularly dangerous or damaging*[44]

It suggests that the higher level of culpability is associated with '*the extreme* risk *posed to Australia's national security in such cases.'* On the face of it the increased risk flowing from these aggravating factors – as distinct from the conduct covered in the underlying offences - might vary from trivial or minor to serious and maybe even extreme.

At least one of the aggravating factors chosen appears to be selected as a deterrent against the potential for whistle-blowers such as Edward Snowden to collect and publish very large amounts of secret information. Although there are varying views as to whether the actions of a Snowden were more beneficial to the public interest than they were harmful to the USA's defence and security, to deter large scale disclosure of secret information is a legitimate objective.

It is however doubtful that ramped up offences and penalties will achieve this in the digital age. Greater benefit might be achieved from greater attention to the technical and administrative data security regimes governments have in place.

Most of the aggravating factors could apply to disclosures and persons far removed from large scale and dangerous leakers or whistle-blowers.

(b)(1)Security classification of secret or above

The problems of the security classification system have been discussed. It is not certain that disclosure of documents with this classification will 'create an extreme risk to Australia's national security'.

(b)(iv) ***'altering a record to remove or conceal its security classification'***

The aggravated conduct of *'altering a record to remove or conceal its security classification'*(b)(iv) would seem appropriately covered by the underlying offence.

[44] (EFI Bill 2017) EM p271

(b)(iii) involves 5 or more records'

The specification of '5 or more records' ((b)(iii)) having a security classification' as sufficient to elevate the offence to an aggravated one seems slight.

(b)(5) Person held an Australian Government security clearance

Australian Government security clearances operate at multiple levels. Some give access to only a very limited set of information, others give broad high level access. This is not a sufficiently discriminating criterion to justify the aggravated penalty.

On balance the CCLs do not support the aggravated offence 122.3. Given the severity of the underlying offences, it should take a major and serious aggravation to trigger the higher offence.

It should be noted that the CCLs have no objection to aggravated offences in principle.

Penalties

The penalties for this offence range from 20 years to 10 years- depending on the underlying offence. Consistent with our earlier comments we consider this an unjustifiably severe penalty. The penalties for the underlying offences should be reduced to align with the ALRC recommendations and the additional penalty for this aggravated offence should be reduced from 5 years to two years.

Recommendation 4

The CCLs recommend that the aggravated offence 122.3 should be removed from the Bill as the aggravating factors and the likely harm that would result from the aggravating conduct are not substantially different from that covered in the underlying offences.

Failing that:

Recommendation 5

The CCLs recommend:

- that the aggravating factors in 122.3 should be reconsidered to ensure they warrant an increased penalty and
- the additional penalty for each of the underlying offences should be reduced from 5 years imprisonment to 2 years.

13 Unauthorised disclosure of information by Commonwealth officers 122.4

The offence at 122.4 replaces the current *Disclosure of information by Commonwealth officers offence* at section 70 of the Crimes Act and, apart from the modernising of the definition of 'information' and 'communication,' largely replicates it. The penalty is 2 years imprisonment which is the same as for the current offence.

> *(1) A person commits an offence if:*
>
> *(a) the person communicates information; and*
>
> *(b) the person made or obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and*
>
> *(c) the person is under a duty not to disclose the information; and*
>
> *(d) the duty arises under a law of the Commonwealth.*
>
> *Penalty: Imprisonment for 2 years.*

This near replication of the current s70 offence ignores the central ALRC recommendation that general secrecy provisions should move away from '*the wide catch-all provisions*' in the current offence and only criminalise the intentional or reckless disclosure of information that will cause harm , or is likely to cause harm to Australia's interests. The ALRC saw this as the central reform of the current offence:

> *'Criminal sanctions should only be imposed where they are warranted—when the disclosure of government information is likely to cause harm to essential public interests—and where this is not the case, the unauthorised disclosure of information is more appropriately dealt with by the imposition of administrative penalties or the pursuit of contractual remedies;'* [45]

The CCLs agree that it is neither compatible with a robust democracy nor beneficial to the public interest that all unauthorised disclosures of information by commonwealth officers should be criminalised and be subject to a penalty of imprisonment regardless of intention or harm factors.

As recommended by the ALRC and the Biggs Committee only intentional disclosure of information which would cause serious harm to Australia's essential interests should be criminalised. This requirement that the harm should be substantial or serious should be made clear in the Bill or in the

[45] (ALRC report 2009) p23

Explanatory Memorandum. Less serious disclosures should be dealt with by disciplinary or administrative procedures.

Recommendation 6

The CCLs recommend that proposed *unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers offence* (122.4) be amended to incorporate intention and harm elements. The harm should be specified as substantial or serious.

14 Duplication and overlap

The three proposed core secrecy offences – *disclosure of inherently harmful information*, *conduct causing harm to Australia's interests* and *unauthorised disclosure of information by Commonwealth officers* – have a high level of duplication in the conduct they criminalise and the areas they cover. This will continue to be so even if the scope of 122.1(1) and 122.1(2) are limited as recommended by the CCLs.

They also overlap with the S35P specific secrecy offence in the ASIO Act –albeit with a different penalty.

This raises the intent of the 'reform 'of the current offences. The Biggs Committee and the ALRC saw reform as focussing more tightly on disclosures of information which caused (substantial not minor or trivial) harm to Australia's essential elements- the latter also tightly defined. This would involve a move away from the 'catch-all' provisions of the current offences. They also argued that in almost all contexts this should involve an element of intention – or recklessness – by the person.

> This would be achieved by drafting a tightly defined general secrecy offence for commonwealth officers and a subsequent disclosures offence for outsiders[46]. Specific secrecy offences should be agency specific and significantly different from the general secrecy offence.

These fundamental drivers of reform seem to have been completely ignored. The proposed package of general secrecy offences does exactly the opposite. It is not surprising that overlap and duplication have emerged as problems.

In the necessary redrafting of these offences the serious issue of duplication and overlap should be addressed with the view of consolidating the offences into one general secrecy offence for insiders and a subsequent disclosure secrecy offence for outsiders.

[46] (ALRC Report 2009) Recommendations 4-1, 5-1, 6-4,6-5.

The most obvious first step in this process would be the removal of the communication of 'inherently harmful information' offence from the Bill.

Recommendation 7

The CCLs recommend that duplication and overlap across the proposed secrecy offences be addressed and in the redrafting consideration be given to consolidating the offences into a general secrecy offence for insiders and a subsequent disclosure secrecy offence for outsiders. As part of this process the communication of 'inherently harmful information' offence should be removed from the Bill

15 Defences 122.5

As the secrecy offences are so broad in their scope and two of the three core offences (122.1, 122.4) have no harm or intention elements, the available defences have a very heavy weight to carry.

The Bill includes a suite of defences to the secrecy offences in this division. These encompass:

i) Powers, functions and duties in a person's capacity as a Commonwealth officer etc. or under arrangement

ii) Information that is already public – with the authority of the Commonwealth

iii) Information communicated to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner

iv) Information communicated in accordance with the Public Interest Disclosure Act 2013

v) Information communicated to a court or tribunal

vi) Information dealt with or held for the purposes of fair and accurate reporting

vii) Information that has been previously communicated

viii) Information relating to a person etc

Some of these defences ensure that individuals will not commit an offence while carrying out official duties or in certain authorised contexts:

- a person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity (s122.5(1)(a));

- the person dealt with, removed or held the information in accordance with an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information(s122.5(1)(b));

- the information is provided to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner for the purpose of them exercising a power, or performing a function or duty (s122.5(3))

  The defence at s122.5(3) only relates to 'communicating' information. It should include 'dealing with information

- the person communicated the information in accordance with the Public Interest Disclosure Act 2013 (s122.5(4))

  This is applicable only to insiders and does not usually result in information which may be in the public interest being disclosed to the public. The defence only relates to 'communicating' information. It should include 'dealing with information.

- the information is communicated to a court or a tribunal whether or not as a result of a requirement.(s 122.5(5)).

  This does not appear to include legal activity relating to these secrecy offences. This should be made explicit.

Recommendation 8

The CCLs recommend that:

- the defences at s s122.5(3) and s 122.5(4) be amended to include 'dealing with information
- the defence at s122.5(5) be amended to include legal activity arising from the proposed secrecy offences

Other defences relate to the status of the information:

Information that is already public – with the authority of the Commonwealth. **s 122.5(2).**

This is an important and necessary defence, but is limited by the specification that the information has already been communicated or made available to the public '*with the authority of the Commonwealth*.'

Information that has been disclosed by whistle-blowers or becomes publicly accessible in any other way is excluded from this defence. It is to be expected that the information that persons such as journalists, health professionals, civil liberties or human rights advocates or whistle-blowers might be prosecuted for, is more likely to come from 'unauthorised' prior publication than from Commonwealth authorised sources.

Information that has been previously communicated **s 122.5(8)**

This provides a defence for communication of information that 'has already been communicated or made available, to the public' (the ***prior publication***). Unlike 122.5(2) it does not restrict the prior publication to one authorised by the Commonwealth. This extends the scope of the information covered in the 'prior publication' defence significantly.

The person must not have obtained the information through being a commonwealth officer or otherwise engaged by a commonwealth entity or through an arrangement to which the commonwealth is a party. (The core defence for commonwealth officers in contained is s 122.5(1).)

This is therefore a defence for 'outsiders' in relation to previously communicated information. (There is also a journalist specific defence at s122.5 (6).) It is a partial response to the ALRC recommendation for separate subsequent disclosure offences and the similar view of the INSLM in the context of his review of S35P of the ASIO Act.

The person must not have been '*involved in the prior publication (whether directly or indirectly' and*

> *(d) at the time of the communication, the person believes that the communication will not cause harm to Australia's interests or the security or defence of Australia; and*
>
> *(e) having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.*

This defence will go some way towards providing protection for outsiders involved in subsequent communication of information under the proposed secrecy offences. However, the combined requirements of (d) and (e) will be a significant constraint on the effectiveness of this defence – particularly as the evidentiary burden sits with the defendant.

The expansive meaning of '*Australia's interests or the security or defence of Australia*' incorporated into the offences will make it difficult to **prove** beyond reasonable doubt that the defendant had

reasonable grounds for believing that no harm will result from the further disclosure. It is not unlikely that (e) could be used to discredit the reliability of whistle-blower sources.

Information dealt with or held for the purposes of fair and accurate reporting s122.5(6)

The journalist's defence provided by s122.5(6) is available where the person dealt with or held the information "in the public interest" **and** "in the person's capacity as a journalist engaged in fair and accurate reporting". The defendant bears the evidential burden.

This is an extremely important defence with a heavy burden, given that the suite of proposed secrecy offences effectively criminalises every aspect of investigative journalism in relation to a greatly expanded range of secret government information including and beyond national security and defence matters.

The Bill does not directly define the terms 'public interest', 'journalist' or 'fair and accurate reporting' thus creating considerable uncertainty around this critical defence.

Journalist definition

With regard to the lack of definition of 'journalist' the explanatory memorandum states:

> *The term 'journalist' should take its ordinary and natural meaning. For example, the Macquarie Dictionary defines 'journalist' as being a person engaged in 'journalism', being 'the business or occupation of writing, editing, and producing photographic images for print media and the production or news and news analysis for broadcast media'. Similarly, the Oxford Dictionary defines 'journalist' as 'a person who writes for newspapers, magazines, or news websites or prepares news to be broadcast'. A journalist need not be regularly employed in a professional capacity, and may include a person who self-publishes news or news analysis*

This could allow a reasonably wide interpretation – it mentions 'websites' 'news to be broadcast' and clarifies that a journalist need not 'be regularly employed in a professional capacity, and may include a person who self-publishes news or news analysis'.

However, it would provide greater certainty and clarity if a wide definition was included in the Bill which incorporated appropriate, contemporary forms of digital journalism and news reporting. This definition should be developed in consultation with practitioners from all modes of contemporary journalism.

Clearly, a fully encompassing definition of 'journalist' is not an easy task. Contemporary professional boundaries are very fluid. The debate as to whether Julian Assange was functioning as a journalist/ publisher or a whistle-blower was not resolved and stands as an example of the complexity and contestability of such a definition.

Notwithstanding – a broader and clearer definition is necessary if this defence is to be available to an appropriate range of 'journalists'.

fair and accurate reporting

It is a specified requirement of the defence that the person dealt with[47] or held the information in their *'capacity as a journalist engaged in fair and accurate reporting*.'

It is well accepted that the issue of determining what is 'fair and accurate 'reporting is subjective and difficult. While there is a good chance of being able to provide evidence of accuracy, a journalist with strong views might be less confident of being able to convince a judge that, on the basis of known facts, that these views are fair.

No standard of "fair and accurate reporting" is directly provided in the Bill. In defamation law, the statutory and common law defences of qualified privilege (which relate to the conduct being reasonable in the circumstances) are notoriously difficult to establish.

The need for clear guidelines as to a standard for 'fair and accurate reporting' is given extra force by the intended interpretation provided by the Explanatory Memorandum:

> *In this context, it is intended that the requirement for the journalist to be engaged in fair and accurate reporting will limit the scope of the defence to journalists who are, in fact, engaged in such reporting, excluding persons who:*
>
> - *merely publish documents or information without engaging in fair and accurate reporting*
> - *use information or documents to produce false or distorted reporting, or*
> - *are not, in fact, journalists engaged in fair and accurate reporting—for example, where the person is an officer or agent of a foreign intelligence service engaged in a foreign interference effort.*[48]

This list significantly limits the definition of 'journalist' and of 'fair and accurate reporting'.

[47] 'deals with' includes 'to communicate' s90.1(1)
[48] (EFI Act 2017. EM) pp281-2

Fair and accurate reporting would normally be understood to exclude biased, distorted and false reporting. But it is more contentious to determine that the 'mere publishing' of documents or information cannot constitute 'fair and accurate' reporting.

It is not clear if this would also exclude publication of documents which have been redacted to exclude harmful information or if a short accompanying comment explaining the significance of the documents would be sufficient to qualify as fair and accurate reporting.

This terminology seems directed at the Wikileaks and Snowden type publication of large amounts of data on the web for public access. It would probably also exclude the publication of the complete Nauru papers for public scrutiny if not the articles analysing aspects of these files. The analytical articles were obviously dependent on the initial data dump of the files into the public arena.

The Explanatory Memorandum indicates that this '*concept of being engaged in fair and accurate reporting is used within section 18D of the Racial Discrimination Act 1975*'[49]. It is of note that the express exemptions in s18D are considerably wider and stronger than that proposed for journalists against secrecy offences in s122.5(6).

> *Section 18C does not render unlawful anything said or done reasonably and in good faith:*
>
> *(c) in making or publishing:*
>
> *(i) a fair and accurate report of any event or matter of public interest; or*
>
> *(ii) a fair comment on any event or matter of public interest if the comment is an expression of a genuine belief held by the person making the comment.*[50]

As they are included as an exception in the protections constructed in this would also provide a higher degree of certainty for journalists wishing to disclose secret government information in the public interest.

The explanation of the intended meaning of ''fair and accurate reporting' in the Explanatory Memorandum should be removed.

The other major problem with this defence is that it is not available to persons other than journalists. If these offences are not going to exercise an unprecedented and unwarranted chill on the public's right to know and to appropriately scrutinise the activities of government, a strong defence has to be available to a much wider range of outsiders including journalists' sources,

[49] ibid

[50] Racial Discrimination Act 1975 section 18D(c). CCLs note that the offence in s18(C) is a civil offence not a criminal offence but the link was made by the Explanatory Memorandum.

academics, members of civil society organizations, and religious groups, political activists, community advocates and ordinary members of the community.

What is needed is a strong, broadly drafted protection relating to disclosures in the public interest.

The CCLs gave extensive consideration to this issue in the context of the extended debates about effective protections for journalists and others in relation to the secrecy offence prohibiting communication of information relating to an ASIO special operation-ASIO Act s35P. [51]

The INSLM's recommendations and the resulting amendment significantly improved the protections for journalists. However, the CCLs consider that notwithstanding these improved protections, S35P will still deter journalists from reporting on ASIO special intelligence operations even where they have evidence that would justify reporting in the public interest. The risk of prosecution is likely to be too great.

General comment on defences

The CCLs acknowledge that these defences are a positive addition to the general secrecy offences.

However, the major issue for the CCLs is the chilling effect of these secrecy offences on fundamental aspects of a robust democracy. Given the unprecedented reach and severity of the offences, it is essential that strong defences are available to significantly ameliorate this impact.

While the suite of defences provides some relevant protections they are too weak to significantly counter this cumulative chill factor in relation to public reporting and the free flow of information relating to government activity.

This is particularly important as all the secrecy offences, apart from 122.4 (unauthorised disclosure by commonwealth officers), apply to third party outsiders as well as commonwealth officers.

The only effective protection would be a major redrafting of the offences to limit their scope and penalties and to incorporate harm and intention elements. In the absence of such redrafting a strong defence is required. This can best be achieved by the inclusion of a general public interest exception.

[51] Eg Joint CCLs submission to the INSLM Review Impact on Journalists of The Operation Of Section 35P of The ASIO Act 1979 22 April 2015.

Recommendation 9

The CCLs recommend that a broad public interest exception be provided for the general secrecy offences in this bill and that a definition of 'public interest' appropriate to these offences be included in the Bill or the Explanatory Memorandum

Failing that:

Recommendation 10

The CCLs recommend:

(i) that a public interest exception for journalists and whistle-blowers be provided for the general secrecy offences in this bill and that a definition of 'public interest' appropriate to these offences be included in the Bill or the Explanatory Memorandum.

(ii) that a broad and contemporary definition of 'journalist' be included in the Bill

(iii) that 122.5(6)(b) *'in the person's capacity as a journalist engaged in fair and accurate reporting'* be deleted .

(iv) that paragraph 1640 in the Explanatory Memorandum limiting the defence at 122.5(6) to 'journalists engaged in fair and accurate reporting' be deleted.

Schedule 1: Treason, Espionage, Foreign Interference and Related Offences

16 National Security – critical definition

It is important that a nation's concept of what is essential to protect its national security is appropriate to the realities of the time. The CCLs accept that changes to the political and legal concept of national security should occur as necessary and that the current global context has called for new approaches to national security.

However the extent and direction of the expansion of the definition of 'national security' at the policy and operational level in recent years has been of ongoing concern to the CCLs . The expansive definition proposed within this Bill in relation to schedule 1 offences is particularly concerning.

National security threats are properly regarded as requiring strong – and if necessary extraordinary – legal responses. The public is willing to allow strong legal protections against threats to national security- such as the creation of specific offences with very serious penalties and the imposition of a high level of secrecy around security related government activity. Previously, in periods of extreme

threat – notably when the country was at war- these extraordinary legal provisions have been ratchetted up – and repealed when no longer needed.

The modern dilemma we must manage is that the major threats to national security are not short-term. The realities of global terrorism and expanding technological capacity for hostile intervention from foreign players are with us for the foreseeable future.

The CCLs argue that this likely state of permanence of high threat means we have to be particularly vigilant about the impact on the fabric of democracy of actions taken to protect national security. If we are not, we are conceding ground that ought not be conceded, and acquiescing to the notion that the values that have underpinned our democratic way of life in Australia are no longer viable.

The conflation of our refugee policy into a national security issue with the attendant ' militarisation' of refugee/immigration agencies and imposition of draconian secrecy provisions -rather than a humanitarian and social policy issue with some security implications- has been a central manifestation of that trend.

A definition of national security that is so broad that it encompasses almost all dimensions of important national activity will inevitably stifle our democracy - because Governments respond to national security threats with extraordinary laws which are not always compatible with a robust democracy.

The continued proliferation of unwarranted and dangerous secrecy provisions relating to the activities of Government and its agencies across many areas will be one key outcome.

The definition of national security provided at s90.4 is very broad and is central to defining the scope of numbers of the offences proposed in this Bill. It is referenced in: the sabotage offences, vulnerability offences, espionage offences, and the foreign interference offences in schedule 1.[52]

*(1) The **national security** of Australia or a foreign country means any of the following:*

(a) the defence of the country;

(b) the protection of the country or any part of it, or the people of the country or any part of it, from activities covered by subsection (2);

[52] s 82.3, s 82.4, s 82.5, s 82.6, s82.7, s 82.8 s91.1(1) and (2), s 91.2(1) and (2), s91.3(1), s91.8(1) and (2)s, 92.2s, 92.3.

(c) the protection of the integrity of the country's territory and borders from serious threats;

(d) the carrying out of the country's responsibilities to any other country in relation to the matter mentioned in paragraph (c) or an activity covered by subsection (2);

(e) the country's political, military or economic relations with another country or other countries

(2) For the purposes of subsection (1), this subsection covers the following activities relating to a country, whether or not directed from, or committed within, the country:

(a) espionage;

(b) sabotage;

(c) terrorism;

(d) political violence;

(e) activities intended and likely to obstruct, hinder or interfere with the performance by the country's defence force of its functions or with the carrying out of other activities by or for the country for the purposes of its defence or safety;

(f) foreign interference.[53].

(a). ***the defence of the country****.* This provision is an appropriate central element of national security.

(b) the protection of the country or any part of it, or the people of the country or any part of it, from activities covered by subsection (2); This provision is an elaboration of (a). The reference to subsection (2) includes activities which are later defined as offences in relation to national security which is somewhat confusing.

(c) ***the protection of the integrity of the country's territory and borders from serious threat.***
This provision would include refugee and asylum seeker activity which while of critical importance - is not appropriately defined and managed as a national security issue.

(d)***the carrying out of the country's responsibilities to any other country in relation to the matter mentioned in paragraph (c) or an activity covered by subsection (2) (d);***
This provision is an extension of (c) – and captures arrangements with other (presumably friendly) countries. As with (c) it is open to a broad interpretation beyond national security.

[53] (E&FI Bill 2017) s90.4

(e)the country's political, military or economic relations with another country or other countries;
The range of matters encompassed in this provision (political, military or economic relations) is very broad. It will include legitimate national security matters such as mutual security and defence arrangements or treaties.

However, the inclusion of 'political' and 'economic' relations is very open-ended. For example, trade agreements- whether protectionist or free trade oriented - may be very important to Australia's interests but do not properly fit with 'national security'. Political relations with other countries may include some aspects which are relevant to national security – but most aspects will be outside a core national security focus.

'**Political violence' 2(d)** is a relevant activity the context of national security but it has a wide definition. Acts of political violence may have no relationship at all with national security.

Where numbers of offences in this Bill are defined in relation to their effect on national security, the scope of conduct captured is affected by the breadth of this very expansive definition. As noted, this applies to sabotage offences, vulnerability offences, espionage offences, and the foreign interference offences in schedule 1.

Recommendation 11

The CCLs recommend that the proposed definition of 'national security' at s90.4 is reviewed to limit its scope more precisely to matters relating to security, defence and limited aspects of international relations. The inclusion of political and economic relations with other countries should be removed from the definition or expressly limited to matters that are central to national security.

Treason and Treachery Offences

17 Treason offences

The Bill updates and combines the two treason offences set out in 80.1AA of the Criminal Code (*Assisting enemies at war with the Commonwealth* and *Assisting countries etc. engaged in armed hostilities against the ADF*) into a single new offence: *Treason—assisting enemy to engage in armed conflict.*

The declared intention is to modernise the terminology to align with the realities of current armed conflict and simplify the structure of treason offences. References to 'war' and 'armed hostilities' are replaced by the more current and flexible definition of 'armed conflict'. [54]

Proposed 80.1AA: Treason—assisting enemy to engage in armed conflict

(1) A person commits an offence if:

*(a) a party (the **enemy**) is engaged in armed conflict involving the Commonwealth or the Australian Defence Force; and*

(b) the enemy is declared in a Proclamation made under section 80.1AB; and

(c) the person engages in conduct; and

(d) the person intends that the conduct will materially assist the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force; and

(e) the conduct materially assists the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force; and

(f) at the time the person engages in the conduct:

(i) the person knows that the person is an Australian citizen or a resident of Australia; or

(ii) the person knows that the person has voluntarily put himself or herself under the protection of the Commonwealth; or

(iii) the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory.[55]

This formulation of the offence achieves the desired simplification and the modernisation of terminology. The penalty of life imprisonment is unchanged.

An unexplained change is the replacement of the current terminology of 'an enemy at war with the Commonwealth' or 'a country or organisation engaged in armed hostilities against the Australian Defence Force' in the current offences56 with the less specific 'involving the Commonwealth or the Australian Defence Force'.

Presumably this vaguer terminology has been used to build in flexibility to accommodate the variety of conflict situations that Australia may be involved in and the variety of roles we may take on in those situations. Quite conceivably there could be situations in which

[54] (EFI Bill 2017 EM) pp27-8

[55] National Security Legislation Amendment (Espionage And Foreign Interference) Bill 2017 . (EFI Bill 2017_ 80.1AA

[56] Criminal Code Act 1995 . 80.1AA (1)(b),(d) and 80.1AA(4)(a)(d)

the Commonwealth or the Australian Defence Forces are not the target of the armed conflict – although they are in some way 'involved' in the situation.

Conversely however, it is difficult to conceive of a situation appropriate to the triggering of a treason offence that could not be captured by maintaining the more specific 'against'.

The Treason offence is clearly intended to be a very serious offence given it attracts the highest penalty. We consider the offence should only be committed in contexts where there is armed conflict with or against our Government or Defence Force and where the conduct concerned has provided assistance to that armed conflict against our Defence Force or Australia. Other offences are available to cover harmful conduct in conflict zones in which the armed conflict is not with/against the Australian Defence Force.

We note that, inconsistent with the above paragraph, the Explanatory Memorandum uses the more specific criteria of armed conflict "against" to explain this section:

The requirement for the Commonwealth to proclaim its enemies for the purpose of the treason offence at section 80.1AA ensures that there is a publicly accessible record of enemies against whom the Commonwealth is engaged in an armed conflict for the purposes of the treason offence at section 80.1AA.*p28*[57]

This more specific and appropriate terminology if adopted into the legislation would also provide a clearer guideline for the basis on which the Governor General can make a Proclamation under proposed 80.1AB:

The Governor General may, by Proclamation, declare a party to be an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force.

Recommendation 12

The CCLs recommend that the proposed treason offence 'assisting enemy to engage in armed conflict' be amended to retain the current requirement that the armed conflict be 'against' the Australian Defence Force or the Commonwealth - s80.1AA (d) and (e)

[57] (EFI Bill 2017 EM) p33.

Recommendation 13

Consistent with recommendation 12, the CCLs also recommend that the Governor General's power to 'declare a party to be an enemy' be on the basis of 'armed conflict against the Commonwealth or the Australian Defence Force.'

18 Proposed s80.1AC Treachery

The current treachery offence in the Crimes Act encompass a range of conduct including: do any act or thing with intent to overthrow the Constitution by revolution or sabotage; assist by any means whatever a proclaimed enemy; instigate a person to make an armed invasion and a range of conduct assisting the enemies of the Australian Defence Force.

221. As the Explanatory Memorandum notes it the language and the offence it creates are 'archaic and antiquated'58.

The Bill replaces part of the current treachery offence 59 with a new offence in the Criminal Code which requires the use of 'force or violence'.

1 A person commits an offence if:

(a) the person engages in conduct; and

(b) the conduct involves the use of force or violence; and

(c) the person engages in the conduct with the intention of overthrowing:

(i) the Constitution; or

(ii) the Government of the Commonwealth, of a State or of a Territory; or

(iii) the lawful authority of the Government of the Commonwealth.[60]

The Penalty is imprisonment for life.

Other parts of the current treachery offence are not replicated in the Bill because they are 'more appropriately dealt with by the laws of the relevant country or through the foreign incursions

[58] (EFI Bill 2017 EM) p 27
[59] Crimes Act 1994 section 24AA(1)(a)(ii) .
[60](EFI Bill 2017) Section 80.1AC

offences in Part 5.5 of the Criminal Code' or are covered by the treason offence in section 80.1AA.[61]

This is a more focussed formulation of the offence. Notwithstanding, the CCLs maintain a concern that (c) (ii) with the reference to states and territories, could still be interpreted widely and cover, for example, prison riots.

It would be useful if the Explanatory Memorandum could provide clarity as to the intended limitation on the interpretation of (c) (ii) by giving some examples of conduct that would not constitute the offence of treachery in these contexts.

The current treachery offences both require an element of intention in relation to conduct.

(1) A person shall not:

(a) do any act or thing ***with intent****:* [62]and

(2) Where a part of the Defence Force is on, or is proceeding to, service outside the Commonwealth and the Territories not forming part of the Commonwealth, a person shall not assist by any means whatever, ***with intent*** *to assist, any persons*[63]

In the new offence only the purpose of the conduct requires 'intent'. The use of 'force or violence' does not require 'intent'.[64]

The Explanatory Memorandum provides a detailed analysis of the fault elements for each element of the offence. In summary:

- Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 80.1AC(1)(a).
  - Section 5.4 of the Criminal Code will apply the fault element for paragraph 80.1AC(1)(b)
  - For paragraph 80.1AC(1)(b), the prosecution will have to prove beyond a reasonable doubt that the person's conduct involved force or violence and that the person was reckless as to this element.
  - For paragraph 80.1AC(1)(c), the prosecution will have to prove beyond a reasonable doubt that the person engaged in his or her conduct with the intention of overthrowing the

[61] (EFI Bill 2017 EM) p34
[62] Crimes Act 1994 section 24AA(1)(a). CCLs emphasis
[63] Crimes Act 1994 section 24AA (2). CCLs emphasis
[64] EFI Bill 2017) Section 80.1AC(c)

Constitution, the Government of the Commonwealth or a State or Territory or the lawful authority of the Government of the Commonwealth.[65]

Given the offence attracts the maximum penalty of life imprisonment, the CCLs do not consider that proof of recklessness is appropriate. Intention to use force and violence should be necessary- as it is in the current offence.

The Explanatory Memorandum does not provide an explanation for this change.

Recommendation 14

Given that the treachery offence attracts the maximum penalty of life imprisonment, the CCLs recommend that intent should be required in relation to 'the use of force or violence' consistent with the current treachery offence.

Recommendation 15

Noting there is uncertainty as to the scope of the offence in relation to the use of force or violence with the intent of overthrowing the governments of the '*Commonwealth, of a State or of a Territory'* 1(c)(ii) the CCLs suggest it would be helpful if clarification is provided in the Explanatory Memorandum .

19 Sabotage Offences

The Bill proposes a range of new sabotage related offences. These offences are graduated by whether they involve a foreign principal and whether the person intended or was reckless as to the result. The penalties range from 15-25 years imprisonment.

It also proposes two levels of the offence of 'introducing vulnerability' - with intention and reckless. The penalties are 15 and 10 years imprisonment.

A new offence of 'preparing for, or planning sabotage' is also proposed with a penalty of imprisonment for 7 years. 66

[65] Ibid paras 183-185,p35
[66] EFI Bill 2017) 82.3, 82.4, 82.5,82.6, 82.7, 82.8, 82.9.

The current sabotage offence focusses on the safety and defence of the Commonwealth and the sabotage of Defence Force related infrastructure:

> ***"act of sabotage "*** *means the destruction, damage or impairment, with the intention of prejudicing the safety or defence of the Commonwealth, of any article:*
>
> *(a) that is used, or intended to be used, by the Defence Force or a part of the Defence Force or is used, or intended to be used, in the Commonwealth or a Territory not forming part of the Commonwealth, by the armed forces of a country that is a proclaimed country for the purposes of section 24AA;*
>
> *(b) that is used, or intended to be used, in or in connexion with the manufacture, investigation or testing of weapons or apparatus of war;*
>
> *(c) that is used, or intended to be used, for any purpose that relates directly to the defence of the Commonwealth; or*
>
> *(d) that is in or forms part of a place that is a prohibited place within the meaning of section 80.*[67]

There have been few, if any, prosecutions under this offence.[68] The ALRC in 2006 recommended that it be included in a review of offences in Part II Crimes Act to determine which offences 'merit retention, modernisation and relocation to the Criminal Code and which offences should be abolished." [69]

The core elements of the new sabotage offences are:

> *(1) A person commits an offence if:*
>
> *(a) the person engages in conduct; and*
>
> *(b) the conduct results in damage to public infrastructure; and*
>
> *(c) the person intends*[70] *that the conduct will:*
>
> *(i) prejudice Australia's national security; or*
>
> *(ii) advantage the national security of a foreign country*[71]*.*

The unlawful conduct under the sabotage offence must result in 'damage to public infrastructure'. Both 'public infrastructure' and 'damage to public infrastructure' are defined.

---

[67] Crimes Act s 24AB(1).

[68] ALRC Fighting Words Report: A review of Sedition Laws in Australia July 2006. (ALRC Sedition Report 2006) p77. There were no prosecutions at the time of this report in 2006.

[69] (ALRC Sedition Report 2006) The ALRC noted that the earlier Gibb report has recommended simplification of this offence and the repeal of related offences

[70] Or ' is reckless as to whether'.

[71] EFI Bill 82.3

The definition of 'public infrastructure' significantly extends the coverage of the sabotage offences beyond damage to defence related infrastructure in the current offence:

> *(1)**Public infrastructure** means any of the following:*
>
> *(a) any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth;*
>
> *(b) defence premises within the meaning of Part VIA of the Defence Act 1903;*
>
> *(c) service property, and service land, within the meaning of the Defence Force Discipline Act 1982;*
>
> *(d) any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act 1997;*
>
> *(e) any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:*
>
> (i) provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind; and
>
> (ii) is located in Australia; and
>
> (iii) belongs to or is operated by a constitutional corporation or is used to facilitate constitutional trade and commerce.[72]

This expanded coverage reflects the realities of technological advances and the resulting new types of critical infrastructure notably telecommunications and other electronic systems. Similar realities and concerns underpin the Security of Critical Infrastructure Bill 2017.

This defining list of 'public infrastructure' for the purpose of sabotage (and other) offences also reflects the reality that much of the nation's 'infrastructure' (including 'critical' infrastructure) is no longer owned by the Commonwealth or states/territories. This Explanatory Memorandum argues:

> *It is essential to cover privately owned infrastructure within the definition of **public infrastructure** because the consequences flowing from damage to these types of infrastructure could be as damaging as damage to infrastructure owned by the Commonwealth.[73]*

However the CCLs are concerned at the breadth of the definition of 'public infrastructure'. This definition conflates infrastructure for sabotage or national security purposes with a very wide range

[72] Ibid *82.2(1)*
[73] EFI Bill 2017.EM p43

of infrastructure owned by the commonwealth or privately. It can be read as including infrastructure which may be neither defence related nor of critical significance on any area eg:

> *'any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that: provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind'*[74]

'***Damage to public infrastructure'*** is reasonably defined in terms of conduct but is linked to the overly broad definition of 'public infrastructure':

> *'conduct results in **damage to public infrastructure** if any of the following paragraphs apply in relation to public infrastructure:*
>
> *(a) the conduct destroys it or results in its destruction;*
>
> *(b) the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable;*
>
> *(c) the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose;*
>
> *(d) the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it;*
>
> *(e) the conduct results in it or any part of it becoming defective or being contaminated;*
>
> *(f) the conduct significantly degrades its quality;*
>
> *(g) if it is an electronic system—the conduct seriously disrupts it.*[75]

The combined impact of the defined scope of 'public infrastructure' and the defined meaning of '**damage** to public infrastructure'[76] could capture conduct of minor significance in terms of actual harm done to the infrastructure or harm to infrastructure that has no significant relationship with an appropriately defined 'national security'.[77]

The Explanatory Memorandum explains the intended meaning of 'the *conduct will prejudice Australia's national security' or 'advantage the national security of a foreign country'*[78].

> *The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to*

[74] EFI Bill s 82.1
[75] (EFI Bill 2017) s 82.1(c)(i)
[76] EFI Bill s 82.1
[77] For example: s 82.1 *(b)the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable;*
[78] EFI Bill 82.3

Australia. The term is also intended to cover impairment or loss to Australia's national security interests. The prejudice to Australia's national security is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice that has no long-lasting effect, nor embarrassment to an Australian person or Australia's people.[79]

This intended meaning- that the harm or prejudice to Australia's national security need not be 'serious or substantial' but cannot be minor or trivial – is unclear. It seems to be suggesting a 'middling' level of harm.

The sabotage offences should be redrafted to ensure that the intended breadth of the provisions is clearly stipulated.

In the view of the CCLs it should be made clear that the level of harm should 'serious or substantial' and that conduct that does not result in substantial or significant 'prejudice' to Australia's national security would be adequately and more appropriately dealt with outside the sabotage offence[80].

The sabotage offences should be redrafted to ensure that it is clearly stipulated.

The conduct of damaging public infrastructure has to be with the intention of– or with recklessness as to– prejudicing Australia's national security or advantaging the national security of a foreign country.[81]

However, the definition of national security is so broadly defined that damage to almost any significant infrastructure could be construed as an act of sabotage.

The CCLs are not aware of substantive explanations as to why the major expansion of the definition of national security and the sabotage offences was seen as necessary. We note that prior reviews recommended the offence be simplified and its scope reduced[82].

There may be a case for including non-defence related infrastructure within the sabotage offence but this should only be critical infrastructure with a direct and significant connection to national security.

The offence should be reconsidered with a view to scaling back its scope.

The requirement that the Attorney General must consent to any prosecution under this offence is supported.

[79] (EFI Bill 2017 EM) pp46-7 and repeated in xx other places. CCLs' emophasis.
[80] For example destroying or damaging Commonwealth property Crimes Act s 29.
[81] EFI Bill 82.3
[82] ALRC cites the Biggs review.

The proposed graduated penalties for the sabotage offences are appropriate – subject to the proposed amendment above.

Recommendation 16

The CCLs recommend that:

i. the definition of 'public infrastructure' at s82.3 should be reviewed with the intention of limiting its scope to include only critical infrastructure with clear connections to national security. The reference to *'(e) any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system)that i) provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind* should be removed or redrafted to limit is meaning to infrastructure of significance to national security;

ii. the meaning of '*prejudice to Australia's national security'* in the context of these sabotage offences should be clarified in the Bill to mean 'serious or substantial'. Paragraph 251 in the Explanatory Memorandum relating to the intended meaning of *prejudice to Australia's national security'* should be appropriately amended;

iii. the proposed sabotage offences - s 82.3, 82.4, 82.5, 82.6 - should not proceed without these amendments.

20 Vulnerability offences

The Bill proposes a new 'introducing vulnerability' offence[83]. This involves conduct which results in an article or thing or software, which is, or is part of, public infrastructure, becoming vulnerable to misuse or impairment or to being accessed or modified by a person not entitled to do so. The person must intend that (or be reckless as to) the conduct will lead to any of the following:

i) prejudice to Australia's national security;

ii) harm or prejudice to Australia's economic interests;

iii) disruption to the functions of the Government of the Commonwealth, of a State or of a Territory;

iv) damage to public infrastructure.

The CCLs accept that there is a need for this offence to capture kinds of harm associated with modern technology.

[83] (EFI Bill 2017)S82.7. The offence with conduct reckless as to is at s82.8

However, the CCLs are concerned with the potential scope of the offence and possibility of conduct which has minor harmful effects to be captured. Any of the four categories of harm listed - *national security, Australia's economic interests, functions of the Government of the Commonwealth, of a State or of a Territory and public infrastructure* - can be interpreted broadly.

In our view 'harm or prejudice to Australia's economic interests' is a particularly expansive and contentious category. There are valid competing understandings of what is, or is not, harmful or beneficial to Australia's economic interests. The CCLs are not convinced this is an appropriate category of harm to be covered by national security offences.

The category of *Australia's economic interests* (82.7(d)(ii) and 82.8(d)(ii) should be removed from the vulnerability offence or redrafted to specific a clearly defined economic interest directly related to national security.

As noted previously the definitions of 'national infrastructure' and 'national security' are overly broad. As these determine the scope of criminal conduct in the vulnerability offences, it is possible that they could capture harm that is not relevant to an appropriately defined national security.

We have previously discussed the problem with the definition of 'prejudice' provided in the Explanatory Memorandum which suggests an interpretation that harm caused in these need not be 'serious or substantial'. The same problem applies for these offences.[84] The term 'prejudice' describes the harm required in relation to 'national security' and 'Australia's economic interests'.

The CCLs consider that given the seriousness of these vulnerability offences, the definition of 'prejudice' should be amended to require 'serious or substantial' harm.

The penalty is 15 years imprisonment and 10 years for the 'reckless as to' offence. These are appropriate – subject to the clarification above as to the seriousness of the harm (prejudice) to Australia's national security and economic interests.

Recommendation 17

[84] (EFI Bill 2017 EM) p.68

The CCLs support the broad intention of the 'introducing vulnerability' offence.

Recommendation 18

The CCLs recommend the vulnerability offences at s82.7 and s82.8 should not proceed until:

i) The category 'harm to Australia's economic functions' is removed or more specifically defined to limit its scope to a clearly defined economic interest, directly related to national security.

ii) the meaning of '*prejudice to Australia's national security'* in the context of these vulnerability offences should be clarified in the Bill to mean 'serious or substantial' harm. Paragraphs 370 and 372 in the Explanatory Memorandum relating to the intended meaning of '*prejudice to Australia's national security'* should be appropriately amended; and

iii) the definitions of 'national security' and 'public infrastructure' are revised to limit their ambit (see Recommendations 11 and 16).

21 Preparing for or planning sabotage offence

The Bill proposes to introduce a 'preparing for or planning sabotage offence'. A person who engages in conduct with the intention of preparing for, or planning, a sabotage offence will commit the offence.[85]

The penalty is imprisonment for 7 years.

The inclusion of a proposed 'preparatory or planning' offence is not supported by the CCLs. We opposed the introduction of an anti-terrorism preparatory offence in 2004[86] on grounds of principle. We maintain our objection to very early precursor offences.

The Explanatory Memorandum provides an explanation as to the purpose of this new offence:

> *The purpose of the offence is to give law enforcement authorities the means to deal with preparatory conduct and enable a person to be arrested before Australia's national security is prejudiced or the national security of a foreign country is advantaged.*[87]

[85] (EFI Bill2017) s82.9
[86] Anti-Terrorism Law 2004
[87] (EFI Bill 2017, EM p69.

In our view the stated purpose can be substantially achieved by surveillance, control and detention powers available to police and security authorities and, for preparatory or planning conduct existing criminal offences exist- including the inchoate offences of attempt and conspiracy..

We note that the fault element is imposed on both elements of the offence which provides some protection from wrongful conviction[88]. However given the legal and practical difficulties of establishing sound evidence in relation to preparatory and planning conduct, we do not share the confident view expressed in the Explanatory memorandum:

> *Given the offences are directed at behaviour at the planning or preparation stage, it is appropriate to impose the fault element of intention on both of the elements of the offence. This will ensure that a person will only be guilty of this offence where there is sufficient evidence that the person intended to prepare for, or plan, a sabotage offence*.[89]

Recommendation 19

230. The CCLs recommend that the proposed offence of 'preparing for or planning sabotage' should not proceed because alternative surveillance and management mechanisms (eg control orders and preventative detention orders) and other offences (eg attempt and conspiracy) are available to authorities to achieve the stated purpose of preventing the person from proceeding with an act of sabotage.

22 Summary of recommendations

Recommendation 1

The CCLs consider that the communication of inherently harmful information offence 122.1(1) is not appropriate for a general secrecy offence and is redundant within this Bill as its categories of 'inherently harmful information' substantially duplicate information covered by other proposed offences at 122.2 and 122.4.

The CCLs recommend it be removed from the Bill.

Failing this**:**

[88] (EFA Bill 2017)
[89] (EFI Bill 2017, EM) p 70.

Recommendation 2

The CCLs recommend:

(i) that the communication of inherently harmful information offence (122.1(1)) be redrafted to include a harm element and to remove the strict liability requirement in relation to 1(b) "*the information is inherently harmful information'*.

(ii) The related offences 122.1(2), 122.1(3), 122.1(4), should be similarly redrafted to align with these changes

(iii) that the maximum penalty for 'the communication of inherently harmful information' offence (s122.1(1)) should be reduced to a maximum of 7 years imprisonment to align with those in the current general secrecy offences and with the penalties proposed by the ALRC. The penalties for the related offences 122.1(2), 122.1(3), 122.1(4) should be similarly aligned.

(iv) that the definition of 'inherently harmful information' at 122.1 be amended as follows:

- that paragraph (a) 'security *classified information'* should be removed from the list of 'inherently harmful information' categories.
- that paragraph (c) 'Information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions' be narrowed in its scope by the removal of the reference to 'a foreign intelligence agency.'
- that paragraph (d) ***'****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****'*** should be redrafted to narrow the agencies or contexts in which the information is likely to be harmful to Australia's essential interests
- that consideration be given to whether paragraph (e) is a redundant category given it is defined as a sub-category of 'security or defence of Australia' at paragraph(b).

Recommendation 3

The CCLs recommend that:

(i) the definition of '*cause harm to Australia's interests'* ss121.1(1) is amended to limit its scope to areas of significance to Australia's national security and essential interests by **the removal of:**

- (a)(ii) '*a contravention of a provision, that is subject to a civil penalty, of a law of the* Commonwealth and

- (e) 'relations between the Commonwealth and a State or Territory' and
- *(*c) harm *or prejudice Australia's international relations in relation to information that was communicated in confidence: i)by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and(ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; and*
- *the words "in any other way' from 121.1 (1)(d)*
- the words 'interfere with' from the definition of '*cause harm to Australia's interests* in 121.1(1)(a) and 121.1(1)(b)

(ii) penalties for the offences in s122.3 be aligned with the ALRC recommendations on penalties for Commonwealth secrecy offences which have as a maximum 7 years imprisonment.

(iii) the 'cause harm to Australia's interests offence ' 122.3 not be supported without these amendments.

Recommendation 4

The CCLs recommend that the aggravated offence 122.3 should be removed from the Bill as the aggravating factors and the likely harm that would result from the aggravating conduct are not substantially different from that covered in the underlying offences.

Failing that:

Recommendation 5

The CCLs recommend that the aggravating factors in 122.3 should be reconsidered to ensure they warrant an increased penalty and the additional penalty for each of the underlying offences should be reduced from 5 years imprisonment to 2 years.

Recommendation 6

The CCLs recommend that proposed *unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers offence* (122.4) be amended to incorporate intention and harm elements. The harm should be specified as substantial or serious.

Recommendation 7

The CCLs recommend that duplication and overlap across the proposed secrecy offences be addressed and in the redrafting consideration be given to consolidating the offences into a general secrecy offence for insiders and a subsequent disclosure secrecy offence for outsiders. As part of this process the communication of 'inherently harmful information' offence should be removed from the Bill

Recommendation 8

The CCLs recommend that:

- the defences at s s122.5(3) and s 122.5(4) be amended to include 'dealing with information
- the defence at s122.5(5) be amended to include legal activity arising from the proposed

secrecy offences

Recommendation 9

The CCLs recommend that a broad public interest exception be provided for the general secrecy offences in this bill and that a definition of 'public interest' appropriate to these offences be included in the Bill or the Explanatory Memorandum

Failing that:

Recommendation 10

The CCLs recommend :

(i) that a public interest exception for journalists and whistle-blowers be provided for the general secrecy offences in this bill and that a definition of 'public interest' appropriate to these offences be included in the Bill or the Explanatory Memorandum.

(ii) that a broad and contemporary definition of 'journalist' be included in the Bill

(iii) that 122.5(6)(b) *'in the person's capacity as a journalist engaged in fair and accurate reporting'* be deleted .

(iv) that paragraph 1640 in the Explanatory Memorandum limiting the defence at 122.5(6) to 'journalists engaged in fair and accurate reporting' be deleted.

Recommendation 11

The CCLs recommend that the proposed definition of 'national security' at s90.4 is reviewed to limit its scope more precisely to matters relating to security, defence and limited aspects of international relations. The inclusion of political and economic relations with other countries

should be removed from the definition or expressly limited to matters that are central to national security.

Recommendation 12

The CCLs recommend that the proposed treason offence 'assisting enemy to engage in armed conflict' be amended to retain the current requirement that the armed conflict be 'against' the Australian Defence Force or the Commonwealth - s80.1AA (d) and (e)

Recommendation 13

Consistent with recommendation 12, the CCLs also recommend that the Governor General's power to 'declare a party to be an enemy' be on the basis of 'armed conflict against the Commonwealth or the Australian Defence Force.'

Recommendation 14

Given that the treachery offence attracts the maximum penalty of life imprisonment, the CCLs recommend that intent should be required in relation to 'the use of force or violence' consistent with the current treachery offence.

Recommendation 15

Noting there is uncertainty as to the scope of the offence in relation to the use of force or violence with the intent of overthrowing the governments of the '*Commonwealth, of a State or of a Territory'* 1(c)(ii) the CCLs suggest it would be helpful if clarification is provided in the Explanatory Memorandum .

Recommendation 16

The CCLs recommend that:

(i) the definition of 'public infrastructure' at s82.3 should be reviewed with the intention of limiting its scope to include only critical infrastructure with clear connections to national security.

The reference to '*(e) any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system)that i) provides or relates to providing the public with utilities or services (including transport of people or*

goods) of any kind hould be removed or redrafted to limit is meaning to infrastructure of significance to national security;

(ii) the meaning of '*prejudice to Australia's national security'* in the context of these sabotage offences should be clarified in the Bill to mean 'serious or substantial'. Paragraph 251 in the Explanatory Memorandum relating to the intended meaning of *prejudice to Australia's national security'* should be appropriately amended;

(iii) the proposed sabotage offences - s 82.3, 82.4, 82.5, 82.6 - should not proceed without these amendments.

Recommendation 17

The CCLs support the broad intention of the 'introducing vulnerability' offence.

Recommendation 18

The CCLs recommend the vulnerability offences at s82.7 and s82.8 should not proceed until:

i) The category 'harm to Australia's economic functions' is removed or more specifically defined to limit its scope to a clearly defined economic interest, directly related to national security.

ii) the meaning of '*prejudice to Australia's national security'* in the context of these vulnerability offences should be clarified in the Bill to mean 'serious or substantial' harm. Paragraphs 370 and 372 in the Explanatory Memorandum relating to the intended meaning of '*prejudice to Australia's national security'* should be appropriately amended; and

iii) the definitions of 'national security' and 'public infrastructure' are revised to limit their ambit (see Recommendations 11 and 16).

Recommendation 19

The CCLs recommend that the proposed offence of 'preparing for or planning sabotage' should not proceed because alternative surveillance and management mechanisms (eg control orders and preventative detention orders) and other offences (eg attempt and conspiracy) are available to authorities to achieve the stated purpose of preventing a person from proceeding with an act of sabotage.

23 Concluding Comments

The joint CCLs support the objective of modernising the Schedule I offences relating to national security and foreign influence. There are elements of the Bill which we are able to support- as is evident from the body of this submission.

However, we are not able to support the passage of the schedule 1 package of offences as they are drafted.

The proposed new and updated offences go beyond the stated objective of modernisation and, it would seem by a mixture of intention and carelessness, significantly extend the scope of the existing offences beyond the protection of defence, national security and essential national interests.

Nor is it always clear that the conduct that is being criminalised under these serious offences will necessarily cause serious and substantial harm to national security- notwithstanding the severe penalties.

Schedule 1 will require a deal of work to fix the evident problems with definitions, inconsistencies and the inappropriate reach of the offences.

The CCL's greatest concerns relate to the secrecy offences in schedule 2 - which have even greater problems at the level of detail and in the cumulative impact of the expanded offences.

The reach of these offences has been greatly expanded, contrary to abundant expert advice over recent years, that we need to reduce the reach of the current 'catch-all' offences and capture only information which could cause serious harm to Australia's essential interests.

These offences will apply to 'outsiders' as well as Commonwealth officers. The penalties are very severe and have been more than doubled for some offences.

The cumulative impact of the proposed secrecy offences on journalists, whistle-blowers , freedom of the press, free flow of information and the capacity to hold government accountable is unprecedented and , in the view of the CCLs, poses a real threat to a Australia's democracy.

The problems with Schedule 2 will not be easy to fix quickly. We welcomed the quick response of the Attorney-General to the early criticism of the secrecy offences, but we are concerned at the suggestion that his proposed amendments would be enough to fix all the serious problems.

If there is urgency to move ahead with the offences in Schedule I, we support those who have argued it should be done separately from Schedule 2.[90]

On the broader front, the CCLs have consistently argued that the Government should urgently address the proliferation of specific secrecy provisions in Commonwealth laws which increasingly erode legitimate journalistic freedom and weaken protections for legitimate whistle-blowers. It is disappointing that the Schedule 2 secrecy proposals could have been developed without any apparent consideration of that larger and integrally related reform agenda.

The following statement from the first INSLM was in the context of the controversy around the S35P ASIO special intelligence operations secrecy offence in 2015. It remains centrally relevant to any consideration of schedule 2 offences:

> *'The very serious policy which isn't addressed by this law is whether, as a society, we want effective shield laws for journalists and comprehensive whistle-blower legislation. They are really big issues which are really not addressed at all by this law or current laws'.* [91]

The joint CCLs trust that these comments will be of assistance to the PJCIS in its assessment of the *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*.

This submission was coordinated by Dr Lesley Lynch, Vice President of the NSW Council for Civil Liberties on behalf of the joint CCLs. The submission was written by Dr Lesley Lynch and Mikah Pajaczkowska-Russell (NSWCCL) on behalf of the CCLs with significant input by the executive members of the joint CCLs.

Contact in relation to this submission:

Dr Lesley Lynch Lesley.lynch@nswccl.org.au; 0416497508

[90] Eg Human Rights Law Centre at the PJCIS public hearing 30/1/18.
[91] ABC Media Watch interview 20/3/15.