Appendix 3

Correspondence

SENATOR THE HON MITCH FIFIELD
DEPUTY LEADER OF THE GOVERNMENT IN THE SENATE
MINISTER FOR COMMUNICATIONS
MINISTER FOR THE ARTS

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6100
PARLIAMENT HOUSE
CANBERRA ACT 2600

Broadcasting Legislation Amendment (Foreign Media Ownership and Community Radio) Bill 2017 – Response to the Parliamentary Joint Committee on Human Rights

Dear Chair Ian

I refer to your letter dated 7 February 2018 in relation to the Parliamentary Joint Committee on Human Rights' (the Committee's) assessment of the Broadcasting Legislation Amendment (Foreign Media Ownership and Community Radio) Bill 2017 (the Bill).

I welcome the opportunity to respond to the Committee's comments and provide the following advice under each.

Committee's comment

1.14 The committee therefore seeks the advice of the minister as to whether the limitation on the right to privacy is proportionate to the stated objective of the measure (including whether the power to determine by legislative instrument the information that must be notified is sufficiently circumscribed, and what safeguards apply relating to the collection, storage and disclosure of personal and confidential information).

Response

Proposed subsections 74F(2), 74H(2), 74J(2) and 74K(2) of the Bill confer on the Australian Communications and Media Authority (ACMA) the power to specify, by legislative instrument, additional information relating to a foreign person that they would need to provide to the ACMA.

This power will provide the ACMA with the capacity to collect any additional information that may be necessary to compile and maintain the proposed Register of Foreign Owners of Media Assets (the Register). This is a reserve power that would be used in exceptional circumstances only, if at all. There are also safeguards in place to ensure that this power will not be exercised in such a way as to be incompatible with international human rights law.

- The power will be exercised by way of a legislative instrument, meaning it will be subject to Parliamentary scrutiny.
- I also expect that the ACMA will consult with the Office of the Australian Information Commissioner before making any such instrument.

Moreover, any additional information sought by the ACMA using this power will relate to the legitimate fulfilment of its functions in relation to the Register, and there is no intention that this reserve power would be used to collect additional personal information. In this regard, it should be noted that the ACMA, as an Australian government agency, is bound by and subject to the provisions of the *Privacy Act 1988* (Privacy Act), which include adherence to the Australian Privacy Principles (APP). Among other things, these principles require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent manner.

The APPs also require the ACMA to take such steps as are reasonable in the circumstances to protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure. In a practical sense, I expect that the ACMA will ensure that access to any personal or commercially sensitive information that it collects will only be accessible by those people performing the administration of the Register and on a strictly 'need to know' basis. I also expect that it will implement robust measures to prevent privacy breaches, which may include the establishment of firewalls, network segmentation, role-based access controls, physical security, and auditing and training of its personnel.

In the event that the ACMA no longer requires the information that it collects, the ACMA is required to take such steps as are reasonable in the circumstances to destroy the information, or to ensure that the information is de-identified. It was not necessary to expressly set out the requirements of the Privacy Act in the Bill given that, as an APP entity, the ACMA is required to adhere to these obligations. Section 13 of the Privacy Act imposes significant penalties for serious interferences with privacy.

The measures contained in the Bill are proportionate and appropriately balance the privacy interests of individuals with the policy objective of transparency that the implementation of the Register aims to achieve.

Comment

1.22 *The committee seeks the advice of the minister as to whether the civil penalty provisions in the bill may be considered to be 'criminal' in nature for the purposes of international human rights law (having regard to the committee's Guidance Note 2), addressing in particular:*

- *whether the nature and purposes of the penalties is such that the penalties may be considered 'criminal';*

- *whether the severity of the civil penalties that may be imposed on individuals is such that the penalties may be considered 'criminal', having regard to the regulatory context; and*

- *if the penalties are considered 'criminal' for the purposes of international human rights law, whether the measure accords with criminal process rights (including specific*

guarantees of the right to a fair trial in the determination of a criminal charge, such as the presumption of innocence (article 14(2)).

Response

The Bill's civil penalty provisions, proposed under subsections 74F(3), 74H(3), 74K(3) and 74K(4), should not constitute a criminal penalty under international human rights law. They are not classified as 'criminal' under Australian law, and are dealt with in accordance with the rules and procedures that apply in relation to civil matters.

The purpose of the penalty is not to punish or deter, but rather to ensure that the Register can be a reliable and current source of information about the levels and sources of foreign investment in Australian media companies at any particular time. It is common practice for non-compliance with government regulation to result in the imposition of an administrative penalty.

Moreover, the penalty does not apply to the public in general, but is restricted to foreign persons in a specific regulatory context, being those foreign persons who are required to provide the ACMA with information prescribed by the Bill. Therefore, the only people captured by these provisions are foreign individuals and body corporates with company interests in excess of two and a half per cent in Australian media companies. This will be predominantly corporate entities who are required to report given the nature of investments in the media industry.

The amounts payable under the civil penalty provisions are reasonable and ensure that there is proportionality between the seriousness of the contravention and the quantum of the penalty sought. The effective operation of the Register will be predicated on the information contained within it being reliable and accurate, and the penalties have been set at a level that should ensure compliance in relation to the Register's reporting obligations. These penalty amounts are consistent with the maximum amount that is generally recommended (one-fifth of the maximum penalty that a court could impose on a person, but which is not more than 12 units for an individual and 60 units for a body corporate).

In relation to the Committee's concerns regarding the penalty provisions applying to each day of contravention, I would note that the ACMA has the capacity to exercise forbearance in determining whether to seek the cumulative penalty payable under the Bill. This would involve the ACMA considering, among other things, the circumstances surrounding the contravention. While the penalty contained in the Bill should not be considered criminal for the purposes of international human rights law, I do note that the Bill preserves the privilege against self-incrimination. This is an important safeguard and protection for entities and persons that may be required to disclose information under the Register.

Thank you for your consideration of these issues.

Yours sincerely

MITCH FIFIELD

21/2/18

THE HON JULIE BISHOP MP

Minister for Foreign Affairs

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Mr Goodenough

Thank you for your letter of 7 February 2018 regarding the human rights compatibility of the *Charter of the United Nations (Sanctions—Democratic People's Republic of Korea) (Documents) Amendment Instrument 2017 (No. 1).*

As noted by the Committee in its *Report 1 of 2018*, this instrument amends the *Charter of the United Nations (Sanctions – Democratic People's Republic of Korea) (Documents) Instrument 2017* (the Documents List). Goods mentioned in the Documents List are incorporated into the definition of 'export sanctioned goods' and 'import sanctioned goods' for the purposes of the *Charter of the United Nations (Sanctions – Democratic People's Republic of Korea) Regulations 2008.*

The Documents List is periodically updated to reflect Australia's obligations under relevant United Nations Security Council resolutions (UNSCRs) to prohibit trade in certain items to North Korea. The Documents List thereby gives effect in Australian law to obligations imposed by UNSCRs.

The Government recognises the need to ensure Australians have sufficient certainty about which goods are subject to sanctions. The documents specified by the Documents List are an internationally accepted reference for those industries, persons and companies that trade in such goods. For example, INFCIRC/254/Part 1 and INFCIRC/254/Part 2 referred to in *Report 1 of 2018,* are the guidelines implemented by the Nuclear Suppliers Group for nuclear-exports and nuclear-related exports aimed at ensuring that nuclear trade for peaceful purposes does not contribute to the proliferation of nuclear weapons or other nuclear explosive devices.

+61 2 6277 7500 Parliament House, Canberra ACT 2600, Australia foreign.minister@dfat.gov.au

In addition, the Department of Foreign Affairs and Trade provides a free service (via the Online Sanctions Administration System) whereby members of the public can submit inquiries about whether a proposed transaction is subject to Australia's sanctions laws. This would include an assessment as to whether a good is an import or export sanctioned good under the Documents List.

In light of these factors, the Government's view is that the instrument is compatible with human rights, including the quality of law test and the right to a fair hearing, the right to a fair trial and the right to liberty.

As requested by the Committee, the statement of compatibility with human rights (SCHR) for the next amending instrument for the Documents List will include a substantive assessment of human rights compatibility along the lines I have described above. I will also amend the SCHR for the *Charter of the United Nations (Sanctions—Democratic People's Republic of Korea) (Documents) Amendment Instrument 2017 (No. 1)* to include such an assessment.

I trust this information is of assistance.

Yours sincerely

Julie Bishop

SENATOR THE HON MATHIAS CORMANN
Minister for Finance
Leader of the Government in the Senate

REF: MC18-000337

Mr Ian Goodenough MP
Chair, Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Chair

I thank the Parliamentary Joint Committee on Human Rights for its consideration of the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017 (the Bill).

The Bill updates and harmonises Commonwealth law regarding political finance, ensuring Australia's most influential political actors are subject to consistent transparency, disclosure and reporting requirements, and are banned from accepting foreign political donations.

These measures are important to maintaining Australians' confidence in the integrity of our political system.

I am pleased to provide the attached response to the questions raised by the Committee in its Report 1 of 2018.

I trust that the information provided is of assistance to the Committee.

Kind regards

Mathias Cormann
Minister for Finance

2 February 2018

Response of the Minister for Finance to the Parliamentary Joint Committee on Human Rights in relation to the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017

Registration requirement for political campaigners, third party campaigners or associated entities

Committee comment

1.55 The preceding analysis raises questions about the compatibility of the registration requirement for political campaigners, third party campaigners or associated entities with the right to freedom of expression, the right to freedom of association, the right to take part in public affairs and the right to privacy.

1.56 The committee therefore requests the advice of the minister as to whether the limitation on these rights is proportionate to the stated objective, in particular whether the registration requirements for political campaigners, third party campaigners and associated entities are sufficiently circumscribed, having regard to the breadth of the definitions of 'political expenditure' and 'associated entities'.

Response

I consider the Bill's requirements are sufficiently circumscribed and proportionate, given the significant public interest in promoting the transparency of our political system. I set out my reasons in relation to registration below, noting that the reasons provided here apply equally to the Committee's other comments on the Bill.

As stated in the Bill's Statement of Compatibility with Human Rights (Statement of Compatibility), registration of key non-party political actors promotes the rights of citizens to participate in elections by assisting them to understand the source of political communication. These key non-party actors are already required to identify themselves in political communications by the *Electoral and Other Legislation Amendment Act 2017* (Authorisation Amendment Act). Registration will complement the Authorisation Amendment Act's transparency reforms by:

a) allowing voters to form a view on the effect of political expenditure; and

b) discouraging corruption and activities that may pose a threat to national security.

Registration with the Australian Electoral Commission will be simple and involve the provision of information readily available to the applicant. No fees will apply.

The Bill narrows the current definition of 'political expenditure', as currently set out in the Authorisation Amendment Act. This definition captures expenditure promoting political views. Whether or not the views or the issue are partisan in nature is immaterial to whether they are political in nature, and therefore the transparency of expenditure used to raise the prominence of such views in public debate is in the public interest.

It is also in the public interest for citizens to be able to identify where an issue is prominent in public debate because its supporters or detractors incurred a significant amount of expenditure. Without such transparency, citizens could reasonably infer that the issue was a priority for government intervention, at the cost of other, perhaps more worthy or pressing, issues.

There are expected to be around 50 entities that will be required to register as a third party or political campaigner, taking historic reporting patterns into account.

With respect to the definition of 'associated entity', new subsection 287H(5) clarifies the meaning of 'associated entity'. I disagree with the Committee's analysis, given the ease of registration and this clarification, that the Bill's registration requirements in relation to associated entities could discourage or prevent people from forming an association.

Civil penalties for failure to register

Committee comment

1.69 The committee draws the attention of the minister to its Guidance Note 2 and seeks the advice of the minister as to whether the civil penalty provisions for failing to register as a political campaigner, third party campaigner or associated entity may be considered to be 'criminal' in nature for the purposes of international human rights law, in particular:

- information regarding the regulatory context in which the civil penalty provisions operate, including the nature of the sector being regulated; and
- the relative size of the pecuniary penalties being imposed in context; and
- information regarding the purpose of the penalties (including whether they are designed to deter or punish); and
- whether the severity of the civil penalties that may be imposed on individuals is such that the penalties may be 'criminal' in nature.

Response

The Bill's registration requirements apply to those who spend significant amounts of money attempting to influence the results of an election, and those associated with registered political parties. Based on historic reporting, around 50 entities are expected to be registered as third parties or political campaigners, and around 200 entities as associated entities. There is likely to be some overlap between these two groups (so it is not accurate to add the two figures). Many of these entities will already be subject to annual reporting requirements under the *Commonwealth Electoral Act 1918.*

The maximum civil penalty amount is lower for third parties due to their lower levels of political expenditure. Lower levels of political expenditure are less likely to distort public debate. Third parties may have comparatively fewer financial resources available to them, or fewer connections with registered political parties. This indicates that a lower penalty amount for third parties would have a similar deterrent effect to the higher amounts applied to political campaigners and associated entities in context.

Civil courts are experienced in making civil penalty orders at levels within the maximum amount specified in legislation to reflect the individual circumstances of a case. As the Bill triggers Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*, subsection 82(6) of that Act applies. This subsection provides that, in determining the pecuniary penalty, the court must take into account all relevant matters including:

(a) the nature and extent of the contravention;

(b) the circumstances in which the contravention took place; and

(c) whether the person has previously been found by a court (including a court in a foreign country) to have engaged in any similar conduct.

The requirement for courts to consider a range of factors makes it unlikely that the maximum penalty would be imposed in each and every instance. Therefore, the relevant consideration in setting a civil penalty amount is the most egregious instances of non-compliance. In the context of the Bill's registration requirements, the most egregious instance of non-compliance could, for example, involve a large, well-funded organisation or wealthy individual deliberately concealing from the public the fact that they were incurring large amounts of political expenditure in order to influence the composition of the legislative and executive arms of the Australian Government. Such an outcome would be potentially very beneficial to the entity or individual and very detrimental to the civil and political rights of Australians more broadly. I therefore consider the penalties are more than justified in context.

Purpose of the penalties
When setting civil pecuniary penalties, deterrence is the primary factor considered (see the High Court's discussion in *Commonwealth v Director, Fair Work Building Industry Inspectorate* [2015] HCA 46 at [55] and [59]). The Bill's civil penalties are intended to deter non-compliance.

Committee comment

1.70 If the penalties were to be considered 'criminal' for the purposes of international human rights law, the committee seeks the advice of the minister as to how, and whether the measures could be amended to accord with criminal process rights including specific guarantees of the right to a fair trial in the determination of a criminal charge such as the presumption of innocence (article 14(2)), the right not to incriminate oneself (article 14(3)(g)), the right not to be tried and punished twice for an offence (article 14(7)) and a guarantee against retrospective criminal laws (article 15(1)).

Response

As set out in the Statement of Compatibility, and taking the Committee's guidance into account, I do not consider the penalties are criminal for the purposes of international human rights law.

Guaranteeing the rights in the Committee's comments in paragraph 1.70 would involve criminalising the requirements.

Restrictions on foreign political donations – Compatibility with the right to a fair trial and fair hearing rights

Committee comment

1.84 The preceding analysis raises questions about the compatibility of the foreign donations restrictions in section 302E and the prohibition on soliciting foreign donations in section 302G with the right to freedom of expression, the right to freedom of association and the right to take part in public affairs. This is because the breadth of the concept of 'political purpose' as it applies to those sections may be insufficiently circumscribed so as to be a proportionate limitation on these rights.

1.85 The committee therefore seeks the advice of the minister as to the proportionality of the foreign donation restrictions as they apply to third party campaigners and political campaigners (in section 302E) and 'any other person' (in section 302G), having regard to the breadth of the concept of 'political purpose' (including whether the measures are sufficiently circumscribed).

Response

Section 302E
I draw the Committee's attention to my above comments in relation to registration requirements relying on the concept of 'political purpose', noting the public interest in this case involves citizens' freedom from undue influence or interference when exercising their right to vote.

Section 302G
Effective anti-avoidance provisions like section 302G are essential to the effectiveness of the foreign donations restrictions. Ineffective provisions cannot be proportional, as they do not achieve the public interest which they intend to promote.

Penalties relating to foreign political donations – Compatibility with the right to a fair trial and fair hearing rights

Committee comment

1.92 The committee draws the attention of the minister to its Guidance Note 2 and seeks the advice of the minister as to whether the civil penalty provisions in relation to the foreign donations restrictions may be considered to be 'criminal' in nature for the purposes of international human rights law, in particular:

- information regarding the regulatory context in which the civil penalty provisions operate, including the nature of the sector being regulated and
- the relative size of the pecuniary penalties being imposed in context;
- information regarding the purpose of the penalties (including whether they are designed to deter or punish); and
- whether the severity of the civil penalties that may be imposed on individuals is such that the penalties may be 'criminal' in nature.

Response

With respect to the regulatory context, I refer the Committee to my previous comments regarding the civil penalties for failure to register as, from an implementation perspective, registration triggers the obligation to comply with the foreign donations ban. This means that the regulatory context is highly similar. However, I draw the Committee's attention to the increasing incidence of foreign interference in domestic political processes reported through the free press as a key consideration for the foreign donations restrictions.

Similarly to the registration requirements, the relative size of the foreign donations penalties has been calibrated according to the deterrent effect in context.

Committee comment

1.93 If the penalties could be considered 'criminal' for the purposes of international human rights law, the committee seeks the advice of the minister as to how, and whether, the measures could be amended to accord with criminal process rights including specific guarantees of the right to a fair trial in the determination of a criminal charge such as the presumption of innocence (article 14(2)), the right not to incriminate oneself (article 14(3)(g)), the right not to be tried and punished twice for an offence (article 14(7)) and a guarantee against retrospective criminal laws (article 15(1)).

Response

As set out in the Statement of Compatibility, and taking the Committee's guidance into account, I do not consider the penalties are criminal for the purposes of international human rights law. Guaranteeing the rights in the Committee's comments in paragraph 1.93 would involve removing the parallel civil penalty, and relying on the Bill's criminal offenses for the foreign donations restrictions.

Reporting of non-financial particulars in returns – Compatibility with the right to privacy

Committee comment

1.101 The preceding analysis raises concerns as to whether the requirement to disclose the name and any political party affiliation of senior staff in returns to the Electoral Commission is compatible with the right to privacy.

1.102 The committee therefore seeks the advice of the minister as to the compatibility of the measure with this right, in particular:

- how the measure is rationally connected to (that is, effective to achieve) the legitimate objective; and
- whether the measure is a proportionate limitation on the right to privacy (including whether the measure is sufficiently circumscribed, and whether there are any less rights-restrictive measures available).

Response

As set out in the Statement of Compatibility, these limitations are justifiable on the basis that they promote transparency of the electoral system. Senior staff of persons and entities covered by these requirements freely choose to play an influential role in public debate. As evidenced by media coverage, there are significant implications and public interest in these matters. Requiring these details to be reported to, and published by, the Australian Electoral Commission is directly connected to the Bill's objective of promoting transparency.

Given the public interest, the measure is a proportionate limitation on the impacted individuals' right to privacy. Many of these individuals are already public figures, and the new requirements serve to consolidate this information and make it more readily accessible to ordinary citizens.

Reporting of non-financial particulars in returns – Compatibility with the right to a fair trial and hearing rights

Committee comment

1.108 The committee draws the attention of the minister to its Guidance Note 2 and seeks the advice of the minister as to whether the civil penalty provisions in reporting of non-financial particulars in returns may be considered to be 'criminal' in nature for the purposes of international human rights law, in particular:

- information regarding the regulatory context in which the civil penalty provisions operate, including the nature of the sector being regulated and the relative size of the pecuniary penalties being imposed in context;
- information regarding the purpose of the penalties (including whether they are designed to deter or punish); and
- whether the severity of the civil penalties that may be imposed on individuals is such that the penalties may be 'criminal' in nature.

Response

With respect to the regulatory context, I refer the Committee to my previous comments regarding the civil penalties for failure to register, as, from an implementation perspective, registration triggers the obligation to report. This means that the regulatory context is very similar.

Similarly to the registration requirements, the relative size of the reporting penalties have been calibrated according to the deterrent effect in context.

Committee comment

1.109 If the penalties could be considered 'criminal' for the purposes of international human rights law, the committee seeks the advice of the minister as to how, and whether, the measures could be amended to accord with criminal process rights including specific guarantees of the right to a fair trial in the determination of a criminal charge such as the presumption of innocence (article 14(2)), the right not to incriminate oneself (article 14(3)(g)), the right not to be tried and punished twice for an offence (article 14(7)) and a guarantee against retrospective criminal laws (article 15(1)).

Response

As set out in the Statement of Compatibility, and taking the Committee's guidance into account, I do not consider the penalties are criminal for the purposes of international human rights law.

Guaranteeing the rights in the Committee's comments in paragraph 1.109 would involve criminalising the requirements.

SENATOR THE HON MITCH FIFIELD
DEPUTY LEADER OF THE GOVERNMENT IN THE SENATE
MINISTER FOR COMMUNICATIONS
MINISTER FOR THE ARTS

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Sl.111
PARLIAMENT HOUSE
CANBERRA ACT 2600

Response to Parliamentary Joint Committee on Human Rights

Dear Mr Goodenough

Thank you for your letter of 7 February 2018 regarding the Parliamentary Joint Committee on Human Rights' (the Committee) assessment of the Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Bill 2018 (the Bill).

The Bill will introduce a federal civil penalty regime targeted at among other things, perpetrators who share intimate images without consent. The regime's civil penalties will allow the Office of the eSafety Commissioner (eSafety Office) to take action to quickly remove intimate images posted online without consent, or to address the threat of intimate images being shared without consent. Penalties of up to $105,000 for individuals and up to $525,000 for corporations can be applied for contraventions of the prohibition.

The Committee, in the *Human rights scrutiny report: Report 1 2018*, sought my advice as to whether the severity of the civil penalties that may be imposed on individuals is such that the penalties may be considered 'criminal' in nature for the purposes of international human rights law.

The Committee also sought my advice as to whether the Bill could accordingly engage criminal process rights (i.e. the rights to a fair trial; not incriminate oneself; not to be tried and punished twice for an offence; and a guarantee against retrospective criminal laws); whether any limitations on these rights imposed by the measures are permissible; and whether measures could be amended to accord with criminal process rights. This letter responds to those comments.

The Statement of Compatibility with Human Rights contained in the current Explanatory Memorandum accompanying the Bill outlines the rationale for the civil penalty amounts and circumstances in which they may apply. It notes that they are reasonable, proportionate and necessary. In line with that statement, I remain satisfied that the civil penalty amounts contained in the Bill are justified due to the significant harm that can be caused to victims of non-consensual sharing of intimate images.

In relation to the Committee's concerns, and taking into account the Committee's Guidance Note 2 on offence provisions, civil penalties and human rights, the following factors also support the view that the penalties are not criminal in nature:

- the penalties included in the Bill are expressly civil and not criminal under Australian law;
- the civil penalties set a maximum, pecuniary-only penalty, with no possibility of imprisonment for contravention of a civil penalty provision;
- non-payment of a civil penalty order does not result in imprisonment;
- the Federal Court and Federal Circuit Court retain discretion both as to whether to issue a civil penalty order, and the specific amounts of the order, up to the maximum amounts under the Bill; and
- in practice, the Bill prescribes a graduated approach of remedies and enforcement mechanisms, and civil penalty orders will only be sought is extreme cases.

Given these factors, which are outlined in more detail below, the Government considers that the penalties are not 'criminal' in nature and therefore do not engage any of the applicable criminal process rights, or require any permissible limitations or amended measures to accord with these rights.

No criminal sanction under domestic Australian law

A contravention of a civil penalty provision does not result in the possibility of imprisonment or resultant criminal record, nor does the non-payment of any civil penalty order. Additionally, the civil penalties are pecuniary only, and are necessarily high as they are intended to change behaviour, acting as a deterrent to those who are tempted to engage in this behaviour.

Maximum penalties

Under the Bill, civil penalty order provisions contained in the *Regulatory Powers (Standards Provisions) Act 2014* are triggered if a person shares an intimate image without consent or threatens to share an intimate image without consent or fails to comply with a removal notice. The penalty amounts are up to $105,000 for a person and up to $525,000 for a corporation.

These penalties are intended to be a strong deterrent to not engage in the sharing of intimate images without consent. They are, however, the maximum penalty amounts that may be awarded and a range of matters must first be considered by the courts before the actual amount is decided (as outlined below).

Court discretion in applying civil penalties

If the eSafety Commissioner decides to pursue a civil penalty he/she must apply to the Federal Court or the Federal Circuit Court. The courts have discretion as to whether to issue a penalty order and will decide on the penalty having regard to any relevant matter, including:

a) the nature and extent of the contravention; and
b) the nature and extent of any loss or damage suffered because of the contravention; and

c) the circumstances in which the contravention took place; and
d) whether the person has previously been found by a court (including a court in a foreign country) to have engaged in any similar conduct.

This discretion means that a perpetrator will not automatically receive the maximum penalty and ensures there are processes in place to ensure that any penalty is proportionate to the contravention.

In addition to the penalties, the Bill gives the eSafety Commissioner the power to first pursue a range of responses if there has been a contravention of the prohibition. These remedies include lighter touch remedies such as informal mechanisms, formal warnings and infringement notices. In practice, the stronger remedies, including civil penalties, are expected to only be used in exceptional cases such as a repeat offender where other remedies have been ineffective.

Consultation

When drafting the Bill, my Department consulted with the Attorney-General's Department and considered the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*. Given the impact that the non-consensual sharing of intimate images can have on victims, the Government remains satisfied that there is sufficient justification for the civil penalty amounts and that they are not 'criminal' in nature for the purposes of international human rights law.

Thank you for providing the opportunity to respond to these issues. I trust this information will be of assistance.

Yours sincerely

MITCH FIFIELD
20/2/18

The Hon Christian Porter MP
Attorney-General

MC18-001618
21 FEB 2018

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600
human.rights@aph.gov.au

Dear ~~Mr Goodenough MP~~ Ian

Thank you for your letter of 7 February 2018 requesting my response to enquiries of the Parliamentary Joint Committee on Human Rights (the Committee) regarding the human rights compatibility of Foreign Influence Transparency Scheme Bill 2017 and the Foreign Influence Transparency Scheme (Charges Imposition) Bill 2017.

I have considered the Committee's assessment of the proposed legislation as set out in its Report 1 of 2018 and enclose responses to the matters that the Committee has raised.

As I have stated publicly, I am open to considering amendments to the proposed legislation. These will be considered in the context of the report of the Parliamentary Joint Committee on Intelligence and Security, which is currently conducting an inquiry into the Foreign Influence Transparency Scheme Bill and is due to report by 23 March 2018.

Thank you again for the opportunity to respond to the Committee's concerns.

Yours sincerely

The Hon Christian Porter MP
Attorney-General

Encl. Response to the Parliamentary Joint Committee on Human Rights Report 1 of 2018 – Foreign Influence Transparency Scheme Bill 2017 and Foreign Influence Transparency Scheme (Charges Imposition) Bill 2017

Response to the Parliamentary Joint Committee on Human Rights
Report 1 of 2018
Foreign Influence Transparency Scheme Bill 2017
Foreign Influence Transparency Scheme (Charges Imposition) Bill 2017

Compatibility of the measure with freedom of expression, freedom of association, the right to privacy and the right to take part in the conduct of public affairs

Committee Comment

1.147 The preceding analysis raises questions as to the compatibility of the proposed foreign influence transparency scheme with the freedom of expression, the freedom of association, the right to take part in the conduct of public affairs, and the right to privacy.

1.148 The committee seeks the advice of the minister as to whether the measure is proportionate to the legitimate objective of the measure, including:

- whether the proposed obligation on persons to register where they act 'on behalf' of a 'foreign principal' is sufficiently circumscribed to ensure that the limitation on human rights is only as extensive as strictly necessary;
- whether the measure is accompanied by adequate safeguards (with particular reference to the exemptions from registration, including the exemption to news media in section 28 of the Bill); and
- in relation to the right to privacy, whether the Secretary's power in section 43(1) to make available to the public 'any other information prescribed by the rules' is sufficiently circumscribed and accompanied by adequate safeguards.

Response

The Committee's report notes that a limitation on human rights may be proportionate if 'sufficiently circumscribed to ensure that it is only as extensive as is strictly necessary to achieve its objective' (paragraph 1.140). In paragraph 1.139 of its report the Committee recognises the objective of the Foreign Influence Transparency Scheme Bill (the Bill) as being legitimate. The objective of the Bill, as stated in the Statement of Compatibility with Human Rights (Statement of Compatibility) at paragraph 21, is:

> to introduce a transparency scheme to enhance government and public knowledge of the level and extent to which foreign sources may, through intermediaries acting on their behalf, influence the conduct of Australia's elections, government and parliamentary decision-making, and the creation and implementation of laws and policies.

The Foreign Influence Transparency Scheme (the Scheme) established by the Bill has been carefully targeted to ensure that it does not unjustifiably impose limitations on human rights. An individual or entity will only be required to register under the Scheme if undertaking a registrable activity on behalf of a foreign principal, and if no relevant exemptions apply. The Scheme is targeted to address those activities most likely to impact upon Australia's political and government systems and processes.

A number of specific circumstances must exist for a person or entity to be required to register. These are:

- the identity of the foreign principal
- the nature of the activities undertaken
- the purpose for which the activities are undertaken, and
- in some cases, whether a person has recently held a senior public position in Australia, such as a former member of Parliament.

The definitions of 'foreign principal' in section 10 and undertaking an activity 'on behalf of' a foreign principal in section 11 need to be sufficiently broad so as to achieve the Scheme's transparency objective. However, these sections do not alone give rise to a requirement to register under the Scheme – additional circumstances must always be present before a requirement to register arises. For example, registrable activities at section 21 of the Bill must be undertaken for the purpose of influencing Australia's political and governmental systems and processes.

The Bill does not apply a 'one size fits all' approach to the requirement to register. For example, donor activity (as defined in section 10) is only registrable when undertaken on behalf of a foreign government, foreign public enterprise or foreign political organisation. A person will not need to register if they are engaging in donor activities on behalf of a foreign businesses and foreign individual. In this way, the application of the Scheme has been limited only to the activities and circumstances most in need of transparency, which is a targeted approach that is proportionate to the legitimate objective of the Scheme.

It is also important to note that a requirement to register with the Scheme does not in any way preclude a person or entity from undertaking a registrable arrangement with a foreign principal, or from undertaking registrable activities on behalf of a foreign principal, provided the person is registered to ensure the activities are transparent. This encourages and promotes the ability of decision-makers and the public to be aware of any foreign influences being brought to bear in Australia's political or governmental processes.

Exemptions

The exemptions in Division 4 of Part 2 of the Bill further limit the Scheme's application. Exemptions established by the Bill include:

- activities undertaken to provide humanitarian aid or assistance (section 24)
- legal advice or representation (section 25)
- diplomatic, consular, United Nations and other relevant staff (section 26)
- certain religious activities (section 27)
- news media (section 28)
- commercial negotiations regarding bona fide business or commercial interests (subsection 29(1)), and
- persons employed by, or operating under the name of, the foreign principal (subsection 29(2)).

The exemption for news media at section 28 serves the important purpose of safeguarding the right to freedom of expression. The exemption applies to activities undertaken on behalf of a foreign business

or foreign individual if the activity is solely, or solely for the purposes of, reporting news, presenting current affairs or expressing editorial content in news media. This exemption ensures that Australian media outlets do not need to register for following the direction of a foreign parent company or foreign owner, and recognises that requiring such entities to register would unjustifiably expand the scope of the Scheme and would be unlikely to add to its transparency objective.

The exemption for news and press services does not apply to state-owned news and press services. There is a public interest in knowing when news and press services are directed by a foreign government to influence Australian governmental and political processes.

The definition of 'communications activity' at section 13 expressly excludes the transmission of information or material by broadcasters and carriage service providers or publication of information or material by print media organisations, if that information or material is produced by another person (see subsections 13(3) and 13(4)). This further safeguards the right to freedom of expression by making it clear that the Scheme's obligations are always placed on the person who has the arrangement with the foreign principal to engage in communications activities, or undertakes communications activities on behalf of the foreign principal, for the purpose of political or governmental influence. Broadcasters, carriage services providers and publishers do not undertake communications activities merely because information is communicated or distributed via their services.

Together with targeted registrable activities, the exemptions seek to ensure that the Scheme remains targeted to those activities most in need of transparency and assists in minimising the regulatory burden of the Scheme. The Bill's registration and transparency requirements do not prevent any person from engaging in any arrangements or activities on behalf of a foreign principal. The Bill requires registration, to inform the Australian Government and the public about the forms and sources of foreign influence in Australia's political and governmental processes. This is appropriate to serve the legitimate transparency objective of the Scheme.

The Bill's registration and reporting obligations should not affect the freedom of the press. Rather than constraining the rights to freedom of expression and opinion, the Bill in fact protects and promote these rights by supporting consumers of news media to be aware of, and understand, any foreign influences behind particular communications activities that are linked to Australia's political and governmental processes.

Right to Privacy

The Bill requires minimal information to be provided by registrants upfront, which helps to safeguard registrants' right to privacy. The information to be collected is limited to that which will be essential for the effective administration of the Scheme (see Division 2 of Part 4 - Register of scheme information), to provide decision-makers and the public with visibility of the foreign influences in Australia's political and governmental processes, and to allow for appropriate investigations into potential non-compliance with the Scheme. Only a subset of information provided will be made publicly available, further safeguarding registrants' right to privacy (see section 43).

The Committee identifies that paragraph 43(1)(c) of the Bill, which provides that the Secretary can make available to the public 'any other information prescribed by the rules' is a potential limitation on the right to privacy. Subsection 43(1) provides that the Secretary must make certain information publicly available in relation to each person registered in relation to a foreign principal, including information prescribed in the rules. Paragraph 43(1)(c) provides flexibility for rules to prescribe

additional information that should be made publicly available which were not foreshadowed at the time of establishment of the Scheme. This is particularly important given the Scheme's primary aim is to provide transparency about foreign influence in Australia's political and governmental processes. Achieving this objective inherently requires information to be made public so that decision-makers and members of the community can access it.

The rules will be legislative instruments under the *Legislation Act 2003* and would be subject to the normal disallowance processes. Any rules will also comply with the *Privacy Act 1988,* and will be guided by the Australian Privacy Principles. The department would consult with the Information Commissioner and relevant stakeholders in the development of rules, to ensure they do not unnecessarily infringe upon the right to privacy.

Additional measures to review the human rights implications of the Bill include provisions providing for an annual report to Parliament on the operation of the Scheme (section 69) and for a review of the Scheme's operation within five years of commencement (section 70). The annual report must be tabled in both Houses of Parliament, providing opportunity for both government and public scrutiny. The review of the Scheme will ensure that the Scheme is operating as intended and strikes an appropriate balance between achieving its transparency objective and the regulatory burden for registrants. Both provisions provide opportunity for the public and Parliament to raise concerns about the Scheme's operation, including in relation to limitations on human rights.

The compatibility of the Scheme with the right to equality and non-discrimination

Committee Comment

1.156 The committee notes that the breadth of the definition of 'foreign principal', coupled with the definition of 'on behalf of' raises concerns that the registration requirement may have a disproportionate negative effect on persons or entities that have a foreign membership base, and could therefore amount to indirect discrimination on the basis of nationality.

1.157 The statement of compatibility does not acknowledge that the foreign influence transparency scheme engages the right to equality and non-discrimination and therefore does not provide an assessment of whether the scheme is compatible with this right.

1.158 The committee therefore seeks the advice of the minister as to the compatibility of the foreign influence transparency scheme with the right to equality and non-discrimination.

Response

The right to equality and non-discrimination is set out at articles 2(1) and 26 of the International Covenant on Civil and Political Rights (ICCPR). Article 2(1) provides that each state undertakes to respect and ensure to all individuals the rights recognised in the ICCPR, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Article 26 provides that all persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

In General Comment No. 18, the UN Human Rights Committee recognised that not every differentiation of treatment will constitute discrimination, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a purpose which is legitimate under the covenant.

It is important to note that the Scheme does not prohibit the involvement of foreign principals, nor those individuals who represent their interests, in Australia's political and governmental processes. It does not target any particular country, nationality or diaspora community. Rather, the Scheme seeks to provide transparency to all Australians about the forms and sources of foreign influence in Australia's government and political processes by all foreign principals.

The Scheme simply imposes a requirement, which applies equally to all registrants regardless of the foreign country involved, that when a person is undertaking activities on behalf of a foreign principal, this is made transparent to the decision-maker and the Australian public, so that they are able to accurately assess the interests being brought to bear in respect of a particular decision or process.

As per the committee's report, the Bill could be interpreted as limiting the right to equality and non-discrimination by requiring registration of those individuals or organisations that undertake certain activities on behalf of a foreign principal for the purpose of political or governmental influence and by establishing distinguishable obligations for former Cabinet Ministers, Ministers, members of Parliament and senior public officials. However, these limitations are reasonable and necessary to achieve the legitimate objective of the Bill, which is described at paragraph 21 of the Statement of Compatibility as being:

> to enhance government and public knowledge of the level and extent to which foreign sources may, through intermediaries acting on their behalf, influence the conduct of Australia's elections, government and parliamentary decision-making, and the creation and implementation of laws and policies.

Activities for the purpose of governmental or political influence

Only certain activities or arrangements to undertake activities on behalf of a foreign principal are registrable under the Scheme.

The activities which attract a requirement to register include parliamentary lobbying, general political lobbying, communications activity, and donor activity. Former members of Parliament, Ministers, Cabinet Ministers and senior Commonwealth public officials may also be required to register under the Scheme, if they are employed by, or act on behalf of, a foreign principal immediately after leaving their public role – it is not necessary that these individuals undertake any of the activities listed above.

An activity is undertaken for the purpose of political or governmental influence if a purpose of the activity is to influence, whether directly or indirectly, any aspect of a process in relation to Australian democratic processes (see section 12).

The Bill has been intentionally drafted so that activities undertaken on behalf of a foreign government will always be registrable, unless an exemption applies. Foreign governments have the potential to exercise greater influence over Australian political and governmental processes, and have the ability to utilise proper diplomatic channels to exert such influence. There is therefore a strong public interest in knowing about activities undertaken on behalf of foreign governments, where they are undertaken outside diplomatic channels.

The Bill does not in any way discriminate on the basis of nationality or a particular political or other opinion. Nor does it seek to prohibit an individual or organisation from having or expressing particular political or other opinions or from having political associations. Instead, the Bill requires individuals and organisations to register where they are undertaking activities that may influence Australia's governmental and political processes on behalf of a foreign principal. This is essential to achieve the legitimate transparency objective of the Scheme.

Activities undertaken by former Cabinet Ministers, Ministers, members of Parliament and senior public officials

Sections 22 and 23 of the FITS Bill create separate registration requirements for recent Cabinet Ministers and recent Ministers, members of Parliament and holders of senior Commonwealth positions. These categories of individuals are also excluded from relying on some of the exemptions available to other persons in Division 4 of Part 2 of the Bill, including the exemptions for religion at section 27 and for news media at section 28.

In creating these specific registration requirements for these categories of individuals, the FITS Bill engages the right to non-discrimination and equality by distinguishing a certain section of the Australian public and establishing legislative provisions that apply only to that section. However, this is reasonable and necessary to support the legitimate transparency purpose of the Scheme.

It is in the public interest to know when recent Cabinet Ministers and recent Ministers, members of Parliament and holders of senior Commonwealth positions undertake activities on behalf of a foreign principal in a short period immediately following the cessation of their role. Such persons have recently occupied significant positions of influence and may have had access to classified and sensitive information concerning Australian government priorities, strategies and interests. They are also likely to have a large number of influential and well-placed contacts at senior government levels, both in the Parliament and the Commonwealth public service, and have a greater ability to access those contacts to influence a political or governmental process on behalf of a foreign principal than other Australians. It is appropriate that those individuals are held to a high degree of accountability.

While the Scheme creates separate obligations for these individuals, it does not prohibit them from entering into arrangements with, or engaging in activities on behalf of, a foreign principal. The Scheme simply establishes registration requirements to ensure the Australian public and government decision-makers are aware of their connection to the foreign principal. This supports the legitimate transparency objective of the Scheme and protects the rights to opinion and freedom of expression, freedom of association and participation in public affairs and elections by encouraging and promoting a political system that is transparent.

The definitions of 'recent Cabinet Minister' and 'recent Minister or member of Parliament' in section 10 are time-limited –the categories are limited to individuals who ceased in that role within the previous three years and no longer hold such a position. Similarly, the definition of 'recent holder of a senior Commonwealth position' in section 10 is limited to persons who held a senior Commonwealth position within the last 18 months and no longer hold that position. A further limitation applies in relation to recent Ministers, members of Parliament and holders of senior Commonwealth positions. Activities undertaken on behalf of a foreign principal are only registrable under section 23 when 'the person contributes experience, knowledge, skills or contacts gained in the person's former capacity as a Minister, member of Parliament or holder of a senior Commonwealth position.'

Accordingly, any limitations on the right to equality and non-discrimination are reasonable, necessary and proportionate to achieve the legitimate transparency objective of the Scheme.

SENATOR THE HON MITCH FIFIELD
DEPUTY LEADER OF THE GOVERNMENT IN THE SENATE
MINISTER FOR COMMUNICATIONS
MINISTER FOR THE ARTS

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6100
PARLIAMENT HOUSE
CANBERRA ACT 2600

National Broadcasters Legislation Amendment (Enhanced Transparency) Bill 2017 – Response to the Parliamentary Joint Committee on Human Rights

Dear Chair Ian

I refer to your letter dated 7 February 2018 in relation to the Parliamentary Joint Committee on Human Rights' (the Committee's) assessment of the National Broadcasters Legislation Amendment (Enhanced Transparency) Bill 2017 (the Bill).

I welcome the opportunity to respond to the Committee's comments and provide the following advice under each.

Committee comments

1.185 The committee notes that the right to privacy is engaged and limited by the measure and the preceding analysis raises questions as to whether it is the least rights-restrictive way of achieving the stated aim.

1.186 The committee therefore requests the advice of the minister as to whether the limitation is proportionate to achieving the stated objectives, including whether there are less rights restrictive ways to achieve the stated objectives, such as:

- *Requiring the ABC and SBS in their annual reports to disclose the number or proportion of female employees and on-air talent earning over $200,000 compared to male employees and on-air talent in the same position; or*

- *Requiring disclosure of de-identified or anonymised information as to the number of employees and on-air talent earning over certain amounts (as specific figures or in pay bands).*

Response

The Committee appears to recognise that, although this Bill may place limitations on the right of privacy, it does so with the intent of serving the following legitimate objectives:

- the objective of ensuring a more detailed scrutiny of this area of high expenditure and for better assessments as to whether the ABC and SBS are efficiently using taxpayers' money; and

- the objective of promoting public transparency and scrutiny and achieving policy outcomes such as reducing the gender salary gap.

The measures in the Bill will require the ABC and SBS to not only be more transparent in reporting how they allocate funding to pay high salaries, but how equitable they are in that allocation – for instance, in respect of male to female salaries.

I note the Committee is concerned that the objectives might be achieved through less restrictive measures. I am of the view that the measures are, in fact, a proportionate response to the objectives, and that the alternatives suggested by the Committee will not ensure these objectives are fully realised.

The alternative of requiring the disclosure of de-identified or anonymised information as to the number of employees and on-air talent earning over certain amounts (as specific figures or in pay bands) would provide for more transparency than is currently the case. However, this approach falls short of achieving the stated transparency outcomes for this measure, and helps to obscure potential gender and age discrimination, unconscious bias, and poor expenditure decisions. It also reduces the capacity for public scrutiny of what should be publicly accessible information. Without transparency, the public loses faith that the ABC and SBS are using funding appropriately and are fair and equitable in doing so. As a taxpayer funded entity, it is appropriate to have this level of transparency.

I consider that, given the enhanced transparency objectives underpinning the Bill, the requirement to publish actual salaries and remuneration is a reasonable and proportionate limitation on the right to privacy.

Thank you for your consideration of these issues.

Yours sincerely

MITCH FIFIELD

27/2/18

The Hon Christian Porter MP
Attorney-General

MC18-001708

14 MAR 2018

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600
human.rights@aph.gov.au

Dear Chair

Thank you for your letter of 14 February 2018 requesting my response to enquiries of the Parliamentary Joint Committee on Human Rights (the Committee) regarding the human rights compatibility of National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (the Bill).

I have considered the Committee's assessment of the Bill as set out in its Report 2 of 2018 and enclose responses to the matters that the Committee has raised.

I also enclose a copy of proposed parliamentary amendments to the Bill which I recently provided to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to assist in its inquiry into the Bill. The proposed parliamentary amendments amend the secrecy offences in Schedule 2 of the Bill to:

- narrow the definitions of inherently harmful information and causes harm to Australia
- create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct, and
- strengthen the defence for journalists at section 122.5(6) by:
    - removing any requirement of journalists to demonstrate that their reporting was 'fair and accurate'
    - ensuring the defence is available where a journalist reasonably believes that their conduct was in the public interest, and
    - clarifying that the defence is available for editorial and support staff as well as journalists themselves.

In addition to these matters, the amendments address the definition of security classification, the breadth of the offence at section 91.3 and the application of strict liability to elements of the offence relating to security classified information.

I am open to considering further amendments to the proposed legislation in the context of the PJCIS report which is due in April 2018.

I trust this information is of assistance to the Committee in finalising its assessment of the Bill.

Thank you again for the opportunity to respond to the Committee's concerns.

Yours sincerely

The Hon Christian Porter MP
Attorney-General

Encl. Response to the Parliamentary Joint Committee on Human Rights Report 2 of 2018 – National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Draft parliamentary amendments to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Response to the Parliamentary Joint Committee on Human Rights

Human rights scrutiny report 2 of 2018

National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Secrecy provisions – compatibility with the right to freedom of expression

Committee Comment

1.37 The committee therefore seeks the advice of the Attorney-General as to:

- how the measures are effective to achieve (that is, rationally connected to) the stated objectives of the bill;
- whether the limitations are reasonable and proportionate to achieve the stated objective (including in relation to the breadth of information subject to the secrecy provisions, the adequacy of safeguards and the severity of criminal penalties); and
- how the measures will interact with existing secrecy provisions such as those under the Border Force Act which has been previously considered by the committee.

1.38 In relation to the proportionality of the measures, in light of the information requested above, if it is intended that the proposed secrecy provisions in schedule 2 proceed, advice is also sought as to whether it would be feasible to amend them to:

- appropriately circumscribe the range of 'inherently harmful information' to which the offence in proposed section 122.1 applies;
- appropriately circumscribe the definition of what information 'causes harm to Australia's interests' for the purposes of section 122.2;
- appropriately circumscribe the definition of 'deals' with information for the purposes of the offences under proposed sections 122.1-122.4;
- appropriately circumscribe the scope of information subject to the prohibition on disclosure under proposed section 122.4 (by, for example, introducing a harm element);
- limit the offences in schedule 2 to persons who are or have been engaged by the Commonwealth as an employee or contractor;
- expand the scope of safeguards and defences (including, for example, a general 'public interest' defence, an unsolicited information defence, a broader journalism defence, and the provision of legal advice defence);
- reduce the severity of the penalties which apply; and
- include a sunset clause in relation to the secrecy provisions in schedule 2.

Response

I have provided amendments to the general secrecy offences in Schedule 2 of the Bill to the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The amended secrecy offences have been carefully scoped to ensure they appropriately cover harmful conduct, often undertaken by

our adversaries to support espionage and foreign interference activity. The amendments to the offences in Schedule 2 ensure the offences are reasonable and proportionate to achieve the objective of protecting Australia from harm, including from espionage and foreign interference.

The changes are summarised below.

- The definition of 'inherently harmful information' will be narrowed by:
    - amending the definition of security classification in section 90.5 (at Item 16 of Schedule 1 of the Bill) and section 121.1 (at Item 6 of Schedule 2 of the Bill) will be amended to mean a classification of TOP SECRET or SECRET, or any other equivalent classification or marking prescribed by the regulations.
    - removing paragraph (d) applying to 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.
- The definition of 'cause harm to Australia's interests' will be narrowed by removing:
    - subparagraph (a)(ii) – interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a provision, that is subject to a civil penalty, of a law of the Commonwealth
    - paragraph (d) – harm or prejudice Australia's international relations in any other way, and
    - paragraph (e) – harm or prejudice relations between the Commonwealth and a State or Territory.
- Separate offences will apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply where:
    - the information has a security classification of SECRET or TOP SECRET and the person is reckless as to this element
    - the communication of the information damages the security or defence of Australia and the person is reckless as to this element
    - the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth and the person is reckless as to this element
    - the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.
- The definition of 'Commonwealth officer' will clarify that the definition does not include officers or employees of, or persons engaged by, the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.
- The defence for journalists will be strengthened by:
    - removing any requirement of journalists to demonstrate that their reporting was 'fair and accurate'
    - ensuring the defence is available where a journalist reasonably believes that their conduct was in the public interest, and

    - clarifying that the defence is available for editorial and support staff as well as journalists themselves.

- Strict liability will be removed from elements of the offences relating to information or articles carrying a security classification.

How the measures meet the objectives of the Bill

It is crucial for the types of information listed in the Bill, as amended, to be protected by general secrecy offences. The Bill seeks to criminalise a range of foreign intelligence activity against Australia, which the Australian Secret Intelligence Organisation (ASIO) assesses is occurring on an unprecedented scale. The existing secrecy offences are inadequate to deter conduct leading up to espionage and foreign interference, and fail to take into account the current operational environment.

Publication and communication of sensitive information substantially raises the risk of foreign actors exploiting that information to cause harm to Australia's interests or to advance their own interests. For example, foreign actors may use the information to build a malicious capability in order to influence a political or governmental process of an Australian government or the exercise of an Australian democratic or political right.

The disclosure of harmful information can erode public confidence in the integrity of Australia's institutions and undermine Australian societal values. It can also jeopardise the willingness of international partners to share sensitive information with Australia.

The general secrecy offences in the Bill complement the espionage and foreign interference offences, both of which require proof of a connection to a foreign principal. The general secrecy offences are an essential part of the overall framework as they ensure the unauthorised disclosure of harmful information, that is made or obtained by the Commonwealth, can be prosecuted even if a foreign principal is not involved, is not yet involved, or the link to a foreign principal cannot be proved beyond a reasonable doubt.

Reasonableness and proportionality

The secrecy offences, as amended, are a reasonable way to achieve the Bill's legitimate objective of protecting Australia from espionage and foreign interference. They are proportionate to the grave threat to Australia's sovereignty, prosperity and national security. My department's submission to the PJCIS Inquiry into the Bill contains further detail at pages 6-7 on the nature and extent of the contemporary threat posed by espionage and foreign interference activity, as well as a number of unclassified case studies at Appendix A.

The definitions of 'inherently harmful information' and information that 'causes harm to Australia's interests' in section 122.1 are limited to information which harms Australia's essential public interests. The offences, as amended, apply more broadly to current and former Commonwealth officers who are subject to particular obligations and requirements as part of their employment. The offences for non-Commonwealth officers are much narrower and will only apply where the information is classified TOP SECRET or SECRET or the person's disclosure of, or dealing with, information causes or will cause harm.

The defences in section 122.5 also limit the circumstances in which a person will be criminally responsible for the secrecy offences, providing appropriate safeguards for freedom of expression. Defences are available for:

- people dealing with information in their capacity as a Commonwealth officer or under arrangement (subsection 122.5(1))
- information that is already public (subsection 122.5(2))
- information communicated to the Inspector-General of Intelligence and Security (IGIS), the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner (subsection 122.5(3)
- information communicated in accordance with the *Public Interest Disclosure Act 2013* (PID Act) (subsection 122.5(4))
- information communicated to a court or tribunal (subsection 122.5(5))
- persons dealing with information in their capacity as a person engaged in reporting news, presenting current affairs or expressing editorial content in news media (subsection 122.5(6))
- information that has been previously communicated (subsection 122.5(8)), and
- information relating to a person (subsection 122.5(9)).

Interaction with existing secrecy offences, including in the Australian Border Force Act 2015

The committee references its 2017 scrutiny report on amendments to the secrecy provisions in the *Australian Border Force Act 2015* (Border Force Act) and seeks comment on how the secrecy offences in the Bill interact with existing secrecy offences.

The purpose of the secrecy provisions in the Bill is to create overarching offences in the Criminal Code, which have a general application. The offences capture dealings with information, which would be likely to cause harm to Australia's interests or national security. It is important that this conduct is adequately captured by the criminal law. This means the offences in the Bill may overlap with more specific secrecy offences in other legislation, and, over time, it may be appropriate for these specific offences to be removed to the extent of the overlap.

The secrecy provisions in the Border Force Act are specific offences that only apply to a person who is, or has been, an 'entrusted person' and they disclose 'Immigration and Border Protection Information,' as defined in section 4(1) of the Border Force Act.

Some of the listed information in the Border Force Act is likely to fall within the categories of 'inherently harmful information' and information that 'causes harm to Australia's interests' or is 'likely to cause harm to Australia's interests' under Division 122 of the Bill. For example, 'information the disclosure of which would or could reasonably be expected to prejudice the security, defence or international relations of Australia' is included in the Border Force Act as 'Immigration and Border Protection Information', as well as in the Bill as 'inherently harmful information.'

However, the Bill also covers information not included in the Border Force Act, for example, in relation to 'information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency' within the definition of 'inherently harmful information.' It is important for dealings of this kind to be captured – unauthorised disclosure has the potential to prejudice investigations and operations, and compromise people's safety.

Whereas the secrecy offences in the Border Force Act apply to 'entrusted persons' (being the Secretary, the Australian Border Force Commissioner and Immigration and Border Protection workers), the secrecy offences in the Bill apply to both Commonwealth officers and non-Commonwealth officers.

Committee comment regarding possible amendments

The committee has sought advice about whether it would be feasible to:

- appropriately circumscribe the range of 'inherently harmful information' to which the offence in proposed section 122.1 applies;
- appropriately circumscribe the definition of what information 'causes harm to Australia's interests' for the purposes of section 122.2;
- appropriately circumscribe the definition of 'deals' with information for the purposes of the offences under proposed sections 122.1-122.4;
- appropriately circumscribe the scope of information subject to the prohibition on disclosure under proposed section 122.4 (by, for example, introducing a harm element);
- limit the offences in schedule 2 to persons who are or have been engaged by the Commonwealth as an employee or contractor;
- expand the scope of safeguards and defences (including, for example, a general 'public interest' defence, an unsolicited information defence, a broader journalism defence, and the provision of legal advice defence);
- reduce the severity of the penalties which apply; and
- include a sunset clause in relation to the secrecy provisions in schedule 2.

These issues are addressed below, by reference to the amendments to the draft Bill circulated to the PJCIS where appropriate.

The definition of 'inherently harmful information'

The committee's concerns with the definition of 'inherently harmful information' related to the breadth of the definitions of 'security classified information' (at paragraph (a)) and 'any information provided by a person to the Commonwealth to comply with another law' (at paragraph (d)).

The proposed amendments to the Bill amend the definition of security classification in sections 90.5 and 121.1. Under the new definition, security classification will mean a classification of TOP SECRET or SECRET, or any other equivalent classification or marking prescribed by the regulations. Consistent with the Australian Government's Information Security Management Guidelines (available at www.protectivesecurity.gov.au), information should be classified as TOP SECRET if the unauthorised release of the information could cause exceptionally grave damage to the national interest. Information should be classified as SECRET if the unauthorised release of the information could cause serious damage to the national interest, organisations or individuals.

The new definition will not allow for lower protective markings to be prescribed in the regulations and will only allow equivalent classifications or markings to be prescribed. This will allow flexibility to ensure the definition can be kept up to date if new protective markings of equivalent seriousness are

introduced, or to ensure information bearing former protective markings of equivalent seriousness can continue to be protected.

It is worth noting that the proposed amendments also remove the provisions that apply strict liability to information that has a security classification. The effect of these amendments is that, in addition to proving that information or article had a security classification, the prosecution will also have to prove that the defendant was reckless as to the fact that the information or article had a security classification. Consistent with section 5.4 of the *Criminal Code Act 1995* (Criminal Code), this will require proof that the person was aware of a substantial risk that the information had a security classification and, having regard to the circumstances known to him or her, it was unjustified to take the risk.

Paragraph (d) of the definition of 'inherently harmful information' will be removed. This paragraph applied to information that was provided by a person to the Commonwealth or an authority of the Commonwealth in order to comply with an obligation under law or otherwise by compulsion of law.

The definition of information which 'causes harm to Australia's interests'

The committee expressed concerns about the breadth of the definition of 'causes harm to Australia's interests', particularly the inclusion of information relating to breaches of Commonwealth law that has a civil penalty (subparagraph (a)(ii)).

The definition of 'cause harm to Australia's interests' will be narrowed in the proposed amendments to the Bill by removing subparagraph (a)(ii) – interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a contravention of a provision, that is subject to a civil penalty, of a law of the Commonwealth.

The amendments will also remove paragraph (d) of the definition – harm or prejudice Australia's international relations in any other way, and paragraph (e) – harm or prejudice relations between the Commonwealth and a State or Territory.

The remaining categories of information covered by the definition of 'cause harm to Australia's interests' all require proof of harm to, interference with, or prejudice to, one of the listed categories. These reflect essential public interests. The Explanatory Memorandum provides further information justifying the inclusion of these categories in paragraphs 1283 to 1301.

The definition of 'deals' with information

The definition of deals in section 90.1 of the Bill has been broadened to cover the full range of conduct that can constitute secrecy and espionage offences. This is to ensure the offences comprehensively addresses the full continuum of criminal behaviour that is undertaken in the commission of espionage offences, and to allow authorities to intervene at any stage.

The penalties for the secrecy offences are tiered to ensure that penalties are commensurate with the seriousness and culpability of offending. The higher penalty will apply where a person actually communicates information. Offences relating to other dealings with information will carry lower penalties. In each case, the fault element of intention will apply to the physical element of the offence that a person communicates or deals with information. Consistent with section 5.2 of the Criminal Code, this means that the person must have meant to engage in the conduct.

Accordingly, the definition of 'deals' is appropriately circumscribed and proportionate to the objective of the Bill.

The scope of information in section 122.4 and introducing a harm element

Section 122.4 replaces and narrows section 70 of the Crimes Act. As stated at paragraph 1274 of the Explanatory Memorandum, it is unclear whether a duty at common law or in equity would be a relevant duty for the purposes of the existing offence. New section 122.4 will only apply where a Commonwealth officer had a duty not to disclose information and that duty arises under Commonwealth law.

Where the Parliament has seen fit to impose a duty on a Commonwealth officer not to disclose information, a breach of such a duty is a serious matter. It is important to note that, in addition to proving that the person is under a duty not to disclose information, the prosecution will also need to prove that the person was reckless as to this element. Consistent with section 5.4 of the Criminal Code, this means that the person will need to be aware of a substantial risk that he or she is under a duty not to disclose the information and, having regard to the facts and circumstances known to him or her, it is unjustifiable to take the risk.

As such, it is not necessary for the offence to require proof of additional harm.

Limit the offences to Commonwealth employees or contractors

The proposed amendments to the Bill address the committee's concerns about the application of many of the secrecy offences to both Commonwealth and non-Commonwealth officers.

The amendments create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct. This recognises that secrecy offences should apply differently to Commonwealth and non-Commonwealth officers given that the former have a higher duty to protect such information and are well versed in security procedures.

Sections 122.1 and 122.2 will only apply to a person who made or obtained the information by reason of being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

New offences in section 122.4A will apply to non-Commonwealth officers who communicate or deal with a narrower subset of information than the offences at sections 122.1 and 122.2.

The new offence at subsection 122.4A(1) will apply where:

- a person intentionally communicates information
- the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person is reckless as to this element
- the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person is reckless as to this element
- any one or more of the following applies:

- the information has a security classification of SECRET or TOP SECRET and the person is reckless as to this
- the communication of the information damages the security or defence of Australia and the person is reckless as to this
- the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth and the person is reckless as to this
- the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

This offence will carry a maximum penalty of 10 years imprisonment, which is lower than the penalty applying to the offences relating to communication of information by current or former Commonwealth officers at subsections 122.1(1) and 122.2(1).

The new offence at subsection 122.4A(2) will apply where:

- a person intentionally deals with information (other than by communicating it)
- the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person is reckless as to this element
- the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person is reckless as to this element
- any one or more of the following applies:
    - the information has a security classification of SECRET or TOP SECRET and the person is reckless as to this
    - the dealing damages the security or defence of Australia and the person is reckless as to this
    - the dealing interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth and the person is reckless as to this
    - the dealing harms or prejudices the health or safety of the Australian public or a section of the Australian public.

This offence will carry a maximum penalty of three years imprisonment, which is lower than the 10 year penalty applying to the offences relating to dealings with information by current or former Commonwealth officers at subsections 122.1(2) and 122.2(2).

The effect of limiting all secrecy offences to Commonwealth employees or contractors would significantly limit the Bill's application and undermine its policy rationale to protect Australia's national security. Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. In the same way as any person can commit espionage, any person can threaten Australia's safety, security and stability through the unauthorised disclosure of harmful information.

Scope of safeguards and defences

The offences have appropriate safeguards and will be further strengthened by changes in the proposed amendments to the Bill. The defence for journalists at subsection 122.5(6) will be strengthened by:

- removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate,' ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and
- clarifying that the defence is available for editorial and support staff as well as journalists themselves.

The inclusion of a general public interest defence is not warranted. In relation to the new secrecy offences for non-Commonwealth officers, it is unlikely that conduct genuinely in the public interest could fall within the parameters of the offences and outside the defences in section 122.5. For example, it is difficult to envisage how the harms listed in subsections 122.4A(1), and listed below, could be within the public interest:

- the information has a security classification of SECRET or TOP SECRET and the person is reckless as to this
- the communication of the information damages the security or defence of Australia and the person is reckless as to this
- the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth and the person is reckless as to this
- the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public

There are established mechanisms for Commonwealth officers to make public interest disclosures under the PID Act and subsection 122.5(4) provides a defence for information communicated in accordance with that Act.

The committee's report raises concerns that a journalist who receives unsolicited information could be liable for a secrecy offence. The fault element of intention always applies to the physical elements of offences involving conduct. Therefore, the prosecution would have to prove beyond reasonable doubt that the journalist intentionally communicated or dealt with the information. Under the amended Bill, if a journalist were to receive unsolicited information, and that information had a security classification, strict liability will no longer apply to the element relating to security classification. This means that, in addition to proving that information or article had a security classification, the prosecution will also have to prove that the defendant was reckless as to the fact that the information or article had a security classification. Consistent with section 5.4 of the Criminal Code, this will require proof that the person was aware of a substantial risk that the information had a security classification and, having regard to the circumstances known to him or her, it was unjustified to take the risk.

It is not intended that the offences cover situations where a person is seeking legal advice about their ability to communicate information or in relation to the application of the offences. A specific defence could provide clarity for such activities.

Penalties

Commonwealth criminal law policy, as set out in the *Guide to Framing Commonwealth Offences* provides that each offence should have a single maximum penalty that is adequate to deter or punish a worst case offence, including repeat offences. The maximum penalty should aim to provide an effective deterrent to the commission of the offence, and should reflect the seriousness of the offence within the relevant legislative scheme.

In the case of the secrecy offences, the disclosure of information could, as a worst case scenario, lead to loss of life. For example, the disclosure of information concerning human sources or officers operating under assumed identities may compromise the safety of those individuals. In light of this worst case scenario, the maximum penalties are considered appropriate. A sentencing court has the discretion to set the penalty at an appropriate level to reflect the relative seriousness against the facts and circumstances of the particular case.

Under the amended Bill, the secrecy offences applicable to Commonwealth officers and non-Commonwealth officers will attract different penalties. This reflects the higher level of culpability on the part of Commonwealth officers who are entrusted by the Australian Government with sensitive information, have a duty to protect such information, and are trained in security procedures. For example, the new offence at subsection 122.4A(1) for non-Commonwealth officers will carry a maximum penalty of 10 years imprisonment, which is lower than the penalty applying to the offences for Commonwealth officers relating to communication of inherently harmful at subsections 122.1(1) and information causing harm to Australia's interests at subsection 122.2(1), both of which attract a maximum penalty of 15 years imprisonment. Similarly the new offence at subsection 122.4A(2) for non-Commonwealth officers who intentionally deal with information will carry a lower penalty than the offences applicable to Commonwealth officers in 122.1(2) and 122.2(2).

Sunset clause

It is appropriate for the general secrecy offences to include a sunset clause, given that their repeal from the statute book would leave disclosure of harmful information without criminal sanction. It would also risk malicious actors structuring their activities around the sunsetting of the offences in order to avoid criminal liability.

If the committee considers it necessary, it would be preferable to provide for a statutory review of the general secrecy offences after a fixed period (for example, five years).

Secrecy provisions – compatibility with the right to an effective remedy

Committee Comment

1.42 The committee therefore seeks the advice of the Attorney-General as to whether the measure is compatible with the right to an effective remedy.

Response

Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights and freedoms recognised by the ICCPR, including the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the State.

While the secrecy offences engage the right to an affective remedy, that right is not limited due to a number of defences in Division 122 which protect disclosure in certain circumstances. These defences concern:

- information communicated to the IGIS, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner under subsection 122.5(3). These agencies provide important oversight of the intelligence community, law enforcement agencies and the public service. It is intended that the general secrecy offences should in no way impinge on the ability of the Inspector-General, the Ombudsman, or the Integrity Commissioner, or their staff, to exercise their powers, or to perform their functions or duties.
- information communicated in accordance with the PID Act under subsection 122.5(4). The PID Act establishes a legislative scheme to investigate allegations of wrongdoing in the Commonwealth public sector and provide robust protections for current or former public officials who make qualifying public interest disclosures under the scheme. It is intended that the general secrecy offences should in no way impinge on the operation of the PID Act.
- information communicated to a court or tribunal under subsection 122.5(5). This will ensure people have the ability to disclose information, including voluntarily, in order to participate in proceedings before a court or tribunal, and
- journalists under subsection 122.5(6). This defence ensures journalists have the ability to disclose information to the public on possible violations of rights where such a disclosure is in the public interest. The amended legislation strengthens the defence for journalists by removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate' and clarifying that the defence is also available for editorial and support staff.

Secrecy provisions – compatibility with the right to be presumed innocent

Committee Comment

1.57 In relation to the strict liability which applies to the element of the offence in proposed section 122.1, the committee therefore requests the advice of the Attorney-General as to:

- whether the limitation is a reasonable and proportionate measure to achieve a legitimate objective (including the scope of application to persons who may not be aware of the security classification; the ability of courts to consider whether a security classification is inappropriate; and any safeguards); and
- if the measure proceeds, whether it would be feasible to amend the proposed section 122.1 to provide a prosecution must not be initiated or continued unless it is appropriate that the substance of the information had a security classification at the time of the conduct.

1.58 In relation to the reverse evidential burdens, the committee requests the advice of the Attorney-General as to:

- whether the limitation is a reasonable and proportionate measure to achieve the stated objective (including why the reverse evidential burdens are necessary and the scope of conduct caught by the offence provisions);
- whether there are existing secrecy provisions that would prevent a defendant raising a defence and discharging the evidential burden, and if so, whether this is proportionate to the stated objective; and

- whether it would be feasible to amend the measures so that the relevant matters (currently in defences) are included as elements of the offence or alternatively, to provide that despite section 13.3 of the Criminal Code, a defendant does not bear an evidential (or legal) burden of proof in relying on the offence-specific defences.

Response

Strict liability – security classified information

As noted above, strict liability will be removed from elements of the offences relating to information or articles carrying a security classification in the proposed amendments to the Bill. This means the prosecution will be required to prove, beyond reasonable doubt, that the information or article had a security classification, and that the defendant was reckless as to whether the information or article had a security classification. Consistent with section 5.4 of the Criminal Code, this means the person will need to be aware of a substantial risk that the information or article carried a security classification and, having regard to the circumstances known to the person, it was unjustifiable to take that risk.

Reverse evidential burdens

The construction of the secrecy offences and specific defences is a reasonable and proportionate measure to achieve the Bill's stated objective of protecting Australia's security and Australian interests.

It is reasonable to reverse the onus of proof in certain circumstances, including where a matter is peculiarly within the knowledge of the defendant and where it would be significantly more difficult and costly for the prosecution to disprove the matter than for the defendant to establish the matter. The justification contained in the Explanatory Memorandum for casting lawful authority as a defence for the espionage and foreign interference offences applies equally to the secrecy offences. For example, in relation to the foreign interference offences, paragraph 1116 states:

> It is appropriate for these matters relating to lawful authority to be cast as defences because the source of the alleged authority for the defendant's actions is peculiarly within the defendant's knowledge. It is significantly more cost-effective for the defendant to assert this matter rather than the prosecution needing to disprove the existence of any authority, from any source.

It would be difficult and more costly for the prosecution to prove, beyond a reasonable doubt, that the person did not have lawful authority. To do this, it would be necessary to negative the fact that there was authority for the person's actions in any law or in any aspect of the person's duty or in any of the instructions given by the person's supervisors (at any level). Conversely, if a Commonwealth officer had a particular reason for thinking that they were acting in accordance with a law or with their duties, it would not be difficult for them to describe where they thought that authority arose. The defendant must discharge an evidential burden of proof, which means pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist (section 13.3 of the Criminal Code).

The reversal of proof provisions are proportionate, as the prosecution will still be required to prove each element of the offence beyond a reasonable doubt before a defence can be raised by the defendant. Further, if the defendant discharges an evidential burden, the prosecution will also be required to disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

Amendments to the draft Bill will be developed to ensure IGIS officials do not bear an evidential burden in relation to the defences in section 122.5 of the Bill. The amendments will also broaden the defences at subsections 122.5(3) and (4) to cover all dealings with information, and clarify that the defences in section 122.5 do not affect any immunities that exist in other legislation.

It would not be appropriate to replace the defences in section 122.5 and instead include additional elements in the secrecy offences. This would mean that in every case the prosecution would need to disprove all of the matters listed in the defences in section 122.5, including for example that:

- the information was not communicated to the IGIS, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner
- the information was not communicated in accordance with the PID Act
- the information was not communicated to a court or tribunal
- the person was not engaged in reporting news, presenting current affairs or expressing editorial content in the news media and did not have a reasonable belief that his or her dealing with the information was in the public interest.

Proving all of these matters beyond reasonable doubt would be burdensome and costly when compared to the approach taken in the Bill of providing defences for the defendant to raise, as appropriate and as relevant to the individual facts and circumstances of the particular case.

Espionage offences – compatibility with the right to freedom of expression

Committee Comment

1.72 The committee therefore seeks the advice of the Attorney-General as to:

- how the measures are effective to achieve (that is, rationally connected to) the stated objectives of the bill; and
- whether the limitations are reasonable and proportionate to achieve the stated objective (including in relation to the breadth and types of information subject to espionage provisions, the scope of the definition of 'national security' and the adequacy of safeguards).

1.73 In light of the information requested above, if it is intended that the espionage offences proceed, advice is also sought as to whether it would be feasible to amend them to:

- appropriately circumscribe the range of information to which the offences apply;
- appropriately circumscribe the definition of what information concerns 'Australia's national interests' where making such information available to a foreign national would constitute a criminal offence;
- appropriately circumscribe the definition of 'deals' with information for the purposes of the espionage offences under proposed section 91.1-91.3;
- appropriately circumscribe the scope of conduct covered by proposed section 91.3 (by, for example, introducing a harm element);
- expand the scope of safeguards and defences; and
- include a sunset clause in relation to the espionage provisions in Schedule 1.

Response

How the measures meet the objectives of the Bill

The proposed espionage offences in Division 91 necessarily cover the full range of espionage conduct being engaged in by Australia's foreign adversaries. The new offences criminalise a broad range of dealings with information, including possessing or receiving, and protect a broader range of information, including unclassified material. The current methodology of Australia's adversaries means that dealings with unclassified information, if accompanied by the requisite intention to harm Australia, can be as damaging as the passage of classified information. It is important to note that dealings with such information are only criminal if the defendant intends, or is reckless as to whether their conduct will, harm Australia's national security. The person will also have to deal with information in a way that makes it available to a foreign principal.

The definition of national security in section 90.4 of the Bill is exhaustive and has been drafted consistent with definitions in other Commonwealth legislation, to ensure it reflects contemporary matters relevant to a nation's ability to protect itself from threats. This includes the definition of 'security' in section 4 of the *Australian Security Intelligence Organisation* (ASIO Act) and the definition of 'national security' in section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act). The NSI Act definition substantially implemented the recommendations of the Australian Law Reform Commission (ALRC) in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report 98, June 2004).

The new offences will not just target the person who discloses the information, but also the actions of the foreign principal who receives the information. This is appropriate to ensure that espionage offences apply to the full suite of harmful conduct designed to harm Australia's national security or advantage the national security of a foreign country. The offences of espionage on behalf of a foreign principal in subdivision B of Division 91 are circumscribed in that the prosecution must prove that the person who received the information did so with an intention to, or reckless as to whether their conduct would, prejudice Australia's national security or advantage the national security of a foreign country.

The new offences in Division 91 will also criminalise soliciting or procuring a person to engage in espionage and will introduce a new preparation or planning offence, which will allow law enforcement agencies to intervene at an earlier stage to prevent harmful conduct occurring. Serious harm can flow from activities which seek to solicit or procure a person to engage in espionage, especially if the foreign principal is successful in obtaining classified information that will prejudice Australia's national security. These offences will allow law enforcement to deal with the conduct at the time it occurs, without the need to wait until an espionage offence is committed or sensitive information is actually passed to a foreign principal.

The proposed amendments to the Bill will narrow the scope of the espionage offence at section 91.3, so that the offence will apply where:

- a person intentionally deals with information or an article
- the person deals with the information or article for the primary purpose of making the information or article available to a foreign principal or a person acting on behalf of a foreign principal

- the person's conduct results or will result in the information being made to a foreign principal or a person acting on behalf of a foreign principal and the person is reckless as to this element, and
- the information or article has a security classification and the person is reckless as to this element.

These amendments ensure that conduct that results in classified information being passed to a foreign principal is punishable as an espionage offence where the person's primary purpose in dealing with the information was to make it available to a foreign principal. The inclusion of this additional element ensures that the offence will not inappropriately cover the publication of information by a journalist whose conduct indirectly makes the information available to a foreign principal, but whose primary purpose is to report news or current affairs to the public.

Reasonableness and proportionality

The espionage offences are a reasonable and proportionate way to achieve the Bill's objectives. The Attorney-General's Department submission to the PJCIS Inquiry into the Bill contains further detail on the nature and extent of the contemporary threat posed by espionage and foreign interference activity, including a number of unclassified case studies.

Espionage can cause severe harm to Australia's national security, compromising Australia's military capabilities and alliance relationships, and can pose a grave threat to Australia's economic stability and wellbeing. The offences are structured to capture the full range of harmful espionage conduct, while also being appropriately circumscribed to ensure they do not capture non-threatening activities. As noted above, the prosecution must prove beyond reasonable doubt that the defendant intended to, or was reckless as to whether their conduct would, harm Australia's national security. The information must also have been made available to a foreign principal. The fault element of intention will apply to the physical element of the offence that a person communicates or deals with the information. Consistent with subsection 5.2(1) of the Criminal Code, this means that the person must have meant to engage in the conduct – mere receipt of information would not necessarily satisfy this fault element.

The offences are appropriately limited by defences in subsection 91.4(1) for dealing with information in accordance with a law of the Commonwealth, in accordance with an arrangement or agreement to which the Commonwealth is party, or in the person's capacity as a public official. It is also a defence under subsection 91.4(2) if the person deals with information that has already been communicated or made available to the public with the authority of the Commonwealth.

The offence in section 91.3 will be narrowed as part of my amendments, which will further ensure the measures in the Bill are a proportionate and reasonable way to meet the Bill's objectives. Conduct that results in classified information being passed to a foreign principal will be punishable under section 91.3 where the person's primary purpose in dealing with the information was to make it available to a foreign principal. The inclusion of this additional element ensures that the offence will not inappropriately cover the publication of information by a journalist whose conduct indirectly makes the information available to a foreign principal, but whose primary purpose is to report news or current affairs to the public. Strict liability will also be removed from the security classification element of the espionage offences in section 91.1 and section 91.3.

Committee comment regarding possible amendments

The committee has sought advice about whether it would be feasible to:

- appropriately circumscribe the range of information to which the offences apply
- appropriately circumscribe the definition of what information concerns 'Australia's national interests' where making such information available to a foreign national would constitute a criminal offence
- appropriately circumscribe the definition of 'deals' with information for the purposes of espionage offences under proposed sections 91.1-91.13
- appropriately circumscribe the scope of conduct covered by proposed section 91.3 (by, for example, introducing a harm element)
- expand the scope of safeguards and defences, and
- include a sunset clause in relation to the espionage provisions in Schedule 1.

These issues are addressed below, by reference to the proposed amendments to the Bill where appropriate.

The range of information to which the offences apply

For the reasons described above, it is appropriate for the espionage offences to apply to a broad range of information, including unclassified material. Activities up to communication of information, such as possession, altering, concealing or receiving, can be damaging in themselves as well as part of a course of conduct leading up to disclosure.

The current methodology of Australia's adversaries means that dealing with unclassified information, if accompanied by the requisite intention to, or recklessness as to whether the conduct will, harm Australia, can be as damaging as the passage of classified information. The fault element of intention will apply to the physical element of the offence that a person communicates or deals with the information.

In relation to the offence in section 91.3, the inclusion of an additional 'primary purpose' element in the amended offence (at paragraph 91.3(1)(aa)) means that conduct will only be punishable under that offence where the person's primary purpose in dealing with the information was to make it available to a foreign principal.

Information concerning Australia's national security

The definition of national security in section 90.4 of the Bill is exhaustive and has been drafted consistent with definitions in other Commonwealth legislation, to ensure it reflects contemporary matters relevant to a nation's ability to protect itself from threats. This includes the definition of 'security' in section 4 of the *Australian Security Intelligence Organisation* (ASIO Act) and the definition of 'national security' in section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act). The NSI Act definition substantially implemented the recommendations of the ALRC in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report 98, June 2004).

The definition of 'deal'

The definition of deal in section 90.1 of the Bill covers the full range of harmful conduct that can constitute espionage and secrecy offences. This is to ensure the offences comprehensively address the continuum of criminal behaviour which may be undertaken in the commission of espionage offences, and allow authorities to intervene at any stage. While the definition of 'deal' is necessarily broad, a person will only be criminally responsible for an espionage offence where every element of the offence is satisfied. For example, a person will only commit an offence under subsection 91.1(1) where he or she deals with security classified information or information concerning Australia's security, and the person intends for the conduct to prejudice Australia's national security or advantage the national security of a foreign country, and this results or will result in the information being made available to a foreign principal.

The fault element of intention will apply to the physical element of the espionage offences that a person communicates or deals with information. Consistent with subsection 5.2(1) of the Criminal Code, this means that the person must have meant to engage in the conduct. The mere receipt of information without intention will not satisfy this element.

The scope of section 91.3

The amendments also narrow the scope of the offence at section 91.3. Under the proposed amendments, section 91.3 will apply where:

- a person intentionally deals with information or an article
- the person deals with the information or article for the primary purpose of making the information or article available to a foreign principal or a person acting on behalf of a foreign principal
- the person's conduct results or will result in the information being made to a foreign principal or a person acting on behalf of a foreign principal and the person is reckless as to this element, and
- the information or article has a security classification and the person is reckless as to this element.

These amendments ensure that conduct that results in security classified information being passed to a foreign principal is punishable as an espionage offence where the person's primary purpose in dealing with the information was to make it available to a foreign principal. Consistent with the definition of 'security classification' in section 90.5 of the amended Bill, this offence will only apply where the information is classified TOP SECRET or SECRET (or an equivalent classification prescribed in the regulations).

The inclusion of this additional element ensures that the offence will not inappropriately cover the publication of information by a journalist whose conduct indirectly makes the information available to a foreign principal, but whose primary purpose is to report news or current affairs to the public.

Sunset clause

It is not appropriate for the espionage offences to include a sunset clause, given that their repeal from the statute book would leave disclosure of harmful information vulnerable to foreign principals by persons intending to, or reckless as to whether their conduct will, prejudice Australia's national

security or advantage the national security of a foreign principal without criminal sanction. It would also risk malicious actors structuring their activities around the sunsetting of the offences in order to avoid criminal liability.

If the committee considers it necessary, it would be preferable to provide for a statutory review of the espionage offences after a fixed period (for example, five years).

Espionage offences – compatibility with the right to be presumed innocent

Committee Comment

1.78 The committee therefore requests the advice of the Attorney-General as to whether the limitation is a reasonable and proportionate measure to achieve a legitimate objective (including the scope of application to persons who may not be aware of the security classification, the ability of courts to consider whether a security classification is inappropriate, and any safeguards).

Response

Strict liability will be removed from elements in espionage offences relating to information of articles with a security classification in the proposed amendments to the Bill. This means the prosecution will be required to prove, beyond reasonable doubt, that the information or article had a security classification, and that the defendant was reckless as to whether the information or article had a security classification. Consistent with section 5.4 of the Criminal Code, this means the person will need to be aware of a substantial risk that the information or article carried a security classification and, having regard to the circumstances known to the person, it was unjustifiable to take that risk.

Espionage offences – compatibility with the right to an effective remedy

Committee Comment

1.81 The committee therefore seeks the advice of the Attorney-General as to whether the measure is compatible with the right to an effective remedy.

Response

While the espionage offences may engage the right to an effective remedy under article 2(3) of the ICCPR, that right is not limited.

It would not be appropriate for victims of human rights violations to seek redress by committing an espionage offence, which would involve intention or recklessness to prejudice Australia's national security or advantage the national security of a foreign country, or dealing with information classified as TOP SECRET or SECRET for the primary purpose of providing the information to a foreign principal under section 91.3.

Foreign interference offences – compatibility with the right to freedom of expression

Committee Comment

1.94 The committee therefore seeks the advice of the Attorney-General as to:

- how the measures are effective to achieve (that is, rationally connected to) the stated objectives of the bill; and
- whether the limitations are reasonable and proportionate to achieve the stated objective (including in relation to the breadth of the offences and adequacy of the safeguards)

1.95 In light of the information requested above, if it is intended that the foreign interference offences proceed, advice is also sought as to whether it would be feasible to amend them to:

- appropriately circumscribe the range of conduct to which the offences apply;
- expand the scope of safeguards and defences; and
- include a sunset clause in relation to the foreign interference provisions in schedule 1.

Response

How the measures meet the objectives of the Bill

The foreign interference offences are rationally connected to the objectives of the Bill, being to protect Australia's security and Australian interests. Foreign actors and intelligence services are increasingly engaged in a variety of foreign interference activities relating to Australia. Foreign interference is characterised by clandestine and deceptive activities undertaken by foreign actors seeking to cause significant harm to Australia's national interests, or to advance their own objectives.

The proposed offences in Division 92 are characterised by conduct that influences Australia's political or governmental processes, interferes in Australia's democratic processes, supports the intelligence activities of a foreign principal or prejudices Australia's national security. The offences also require proof that the defendant's conduct was covert or deceptive, involved threats or menaces or targeted a person without disclosing the nature of the defendant's connection to a foreign principal. In combination, this conduct poses threats to Australia's safety and security.

Reasonableness and proportionality

The foreign interference offences are a reasonable way to achieve the Bill's legitimate objectives. The offences are proportionate to the serious threat to Australia's sovereignty, prosperity and national security posed by foreign interference activities. The Attorney-General's Department submission to the PJCIS Inquiry into the Bill contains further detail on the nature and extent of the contemporary threat posed by espionage and foreign interference activity, including a number of unclassified case studies.

It is appropriate to define foreign principal broadly to include public international organisations. This is consistent with the definition in section 70.1 of the Criminal Code. It is appropriate that the foreign interference offences cover such organisations, which may include civil society organisations, as a person could equally seek to interfere in Australia's democratic processes or prejudice Australia's national security on behalf of such actors in some circumstances. The conduct described by the committee at paragraph 1.90 would not necessarily fall within the proposed foreign interference offences. The person must have intentionally failed to disclose their collaboration with a public

international organisation, and been reckless as to influencing the political process. This will require the person to have been aware of a substantial risk that their conduct would influence the political process and, having regard to the circumstances known to him or her, it was unjustified to take the risk.

The committee has expressed concerns in relation to the offences for providing support to foreign intelligence agencies in sections 92.7 and 92.8. However, the word 'support' is narrower than suggested by the committee. As stated in the Explanatory Memorandum at paragraph 1061, the term 'support':

> is intended to cover assistance in the form of providing a benefit or other practical goods and materials, as well as engaging in conduct intended to aid, assist or enhance an organisations activities, operations or objectives.

The offences are modelled on the terrorist organisation offences in the Criminal Code. It is also a requirement of these offences that the prosecution prove beyond reasonable doubt that the person intended to provide support to an organisation and that the person knows, or is reckless as to whether, the organisation is a foreign intelligence agency.

The offences are further circumscribed by defences in section 92.11 for dealing with information in accordance with a law of the Commonwealth, in accordance with an arrangement or agreement to which the Commonwealth is party, or in the person's capacity as a public official.

It would not be appropriate to include additional defences, for example, to excuse foreign interference on the basis that it is 'in the public interest.' Noting the elements of the offence, it is unlikely that conduct that within the scope of the foreign interference offences could be said to also be 'in the public interest'.

Sunset clause

It is not appropriate for the foreign interference offences to include a sunset clause, given that the purpose of the Bill is to fill the current gap in the criminal law, which is contributing to a permissive operating environment for malicious foreign actors engaging in foreign interference activities in Australia. It would also risk malicious actors structuring their activities around the sunsetting of the offences in order to avoid criminal liability.

If the committee considers it necessary, it would be preferable to provide for a statutory review of the espionage offences after a fixed period (for example, five years).

Presumption against bail – compatibility with the right to be released pending trial

Committee Comment

1.107 The committee seeks the advice of the Attorney-General as to:

- how the measure is effective to achieve (that is, rationally connected to) its stated objective (including whether offences to which the presumption applies create particular risks while a person is on bail);
- whether the limitation is a reasonable and proportionate measure to achieve the stated objective including:

- why the current balancing exercise undertaken by bail authorities and courts is insufficient to address the stated objective of the measure;
- whether less rights restrictive alternatives are reasonably available (such as adjusting criteria to be applied in determining whether to grant bail rather than a presumption against bail);
- the existence of adequate and effective safeguards to ensure a person is not deprived of liberty where it is not reasonable, necessary and proportionate in all the circumstances; and
- advice as to the threshold for rebuttal of the presumption against bail including what is likely to constitute 'exceptional circumstances' to justify bail.

Response

A presumption against bail is appropriate for the offences in Division 80 and 91 of the Criminal Code and the foreign interference offences in subsections 92.2(1) and 92.3(1) where it is alleged that the defendant's conduct involved making a threat to cause serious harm or a demand with menaces. The offences that are subject to a presumption against bail are very serious offences. The presumption against bail will limit the possibility of further harmful offending, the communication of information within the knowledge or possession of the accused, interference with evidence and flight out of the jurisdiction. Communication with others is particularly concerning in the context of the conduct targeted by these offences.

The existing espionage, treason and treachery offences are currently listed in subparagraph 15AA(2)(c) of the *Crimes Act 1914* (Crimes Act) – inclusion of offences in Division 80 and 91 merely updates subparagraph 15AA(2)(c) given that the existing offences are being repealed. For these offences, it is important to note that, consistent with subparagraphs 15AA(2)(c)(i) and (ii), the presumption against bail will only apply if the person's conduct is alleged to have caused the death of a person or carried a substantial risk of causing the death of a person.

For the foreign interference offences in subsections 92.2(1) and 92.3(1), the presumption against bail will only apply where it is alleged that any part of the conduct the defendant engaged in involved making a threat to cause serious harm or a demand with menaces. This limitation recognises the significant consequences for an individual's personal safety and mental health if the conduct involves serious harm (consistent with the definition of 'serious harm' in the Dictionary to the Criminal Code) or making a 'demand with menaces' (as defined in section 138.2 of the Criminal Code).

For offences subject to a presumption against bail the accused will nevertheless be afforded to opportunity to rebut the presumption. Further, the granting or refusing of bail will always be at the discretion of the judge hearing the matter.

Telecommunications and serious offences – compatibility with the right to privacy

Committee Comment

1.120 The committee therefore requests the advice of the Attorney-General as to:

- whether the expanded definition of 'serious offence' in the context of existing provisions of the TIA Act constitutes a proportionate limit on the right to privacy (including why allowing warranted access for the investigation of each criminal offence is necessary; who or what

devices could be subject to warranted access; and what safeguards there are with respect to the use, storage and retention of telecommunications content); and

- whether an assessment of the TIA Act could be undertaken to determine its compatibility with the right to privacy.

Response

Serious offence

The offences are appropriately included as 'serious offences' for the purpose of the powers contained in the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Including the proposed offences within the remit of the TIA scheme will allow agencies listed in the TIA Act, in prescribed circumstances and subject to appropriate authorisation processes, to intercept communications, access stored communications and access telecommunications data.

It is important for such agencies to have appropriate powers to investigate each offence, including under the TIA Act. The covert and hidden nature of the conduct targeted by the offences can make them more difficult to detect and investigate through other means. By their nature, espionage and foreign interference often involve complex networks of people, technological sophistication and avoidance of paper and traceable communications. Approved interception of and access to telecommunications information would complement the range of other investigative options available to agencies in investigating these offences.

The seriousness of each offence, coupled with the ability for malicious actors to use electronic means to further conduct in support of the offences, justifies the inclusion of the proposed offences in the definition of 'serious offence' in the TIA Act. The seriousness of each suite of offences, and the gravity of the consequences of the conduct they criminalise, is outlined below:

- Sabotage offences (Division 82): The sabotage offences criminalise conduct causing damage to a broad range of critical infrastructure, including any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth or that is located in Australia and the provides the public with utilities and services. The offences also capture damage to any part of the infrastructure of a telecommunications network. They are necessarily included in the definition of 'serious offence' under the TIA Act because of the serious implications for business, governments and the community disruption to public infrastructure could have.
- Other threats to security – advocating mutiny (Division 83): Mutiny has potentially significant consequences for the defence of Australia. The primary responsibility of the Australian Defence Force is to defend Australia and Australia's interests. By seeking to overthrow the defence force of Australia, acts of mutiny clearly threaten Australia's national security and public order.
- Other threats to security – assisting prisoners of war to escape (Division 83): Assisting prisoners of war can undermine Australia's defence and national security, especially as escaped prisoners may provide assistance to a foreign adversary and cause harm to public safety.
- Other threats to security – military-style training (Division 83): The military-style training offence criminalises the provision, receipt or participation in military-style training where the training is provided on behalf of a foreign government. The offence seeks to ensure that

foreign countries are unable to marshal forces within Australia, which could pose extremely serious threats to the defence and security of Australia.

- Other threats to security – interference with political rights and duties (Division 83): Conduct that interferes with political rights and duties, and involves the use of force, violence, intimidation or threats, is a grave threat to Australia's democracy, undermines public confidence in institutions of government and stifles open debate which underpins Australia's democratic society.
- Espionage (Division 91): The espionage offences criminalise dangerous and harmful conduct aimed at prejudicing Australia's national security or advantaging the national security of a foreign country. Acts of espionage have the potential to diminish public confidence in the integrity of political and government institutions, compromise Australia's military capabilities and alliance relationships, and undercut economic and business interests within Australia and overseas.
- Foreign interference (Division 92): These offences criminalise harmful conduct undertaken by foreign principals to damage or destabilise Australia's system of government and political process, to the detriment of Australia's interests or to create an advantage for the foreign country. Foreign interference involves covert, deceptive or threatening actions by foreign actors who intend to influence Australia's democratic or government processes or to harm Australia, and can be severely damaging to Australia's security and national interests.
- Theft of trade secrets involving foreign government principal (Division 92A): The theft of trade secrets offence seeks to combat the increasing threat of data theft, business interruption and economic espionage, by or on behalf of foreign individuals and entities. Interference in Australia's commercial dealings and trade relations by or on behalf of foreign governments can have serious consequences for Australia's national security and economic interests.
- Aggravated offence for giving false or misleading information (Section 137.1A): A person who succeeds in obtaining or maintaining an Australian Government clearance on the basis of false or misleading information may gain access to highly classified or privileged information. If the person seeks to communicate or deal with that information in an unauthorised manner, including by passing it to a foreign principal, this could significantly damage Australia's national security.
- Secrecy of Information (Division 122): Disclosure of inherently harmful information or information that causes harm to Australia's interests can have significant consequences for Australia's national security, in particular if that information is advantageous to a foreign principal's national security and support espionage and foreign interference activities.

Proportionality

Including the offences within the TIA Act scheme is a proportionate means to achieve the Bill's legitimate objectives.

Under Chapter 2 of the TIA Act, interception warrants may be issued in respect of a person's telecommunications service, if they would be likely to assist an investigation of a serious offence in which either that person is involved, or another person is involved with whom the particular person is likely to communicate using the service. If there are reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service, the issuing judge may issue a warrant in respect of the named person, allowing access to communications made

using a service or device. In both cases, the judge must have regard to the nature and extent of interference with the person's privacy, the gravity of the conduct constituting the offence, the extent to which information gathered under the warrant would be likely to assist an investigation, and other available methods of investigation.

Under Chapter 3 of the TIA Act, stored communications warrants may be issued in respect of a person. Such warrants allow an agency, subject to any conditions and restrictions specified in the warrant, to access a stored communication that was made by the person in respect of whom the warrant was issued, or that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued. A judge or AAT member can only issue a warrant if there are reasonable grounds for suspecting that a particular carrier holds the stored communications, and information gathered under warrant would be likely to assist in the agency's investigation of a serious contravention in which the person is involved. A serious contravention is defined in section 5E of the TIA Act to include a serious offence, as well as offences punishable by imprisonment of at least 3 years and offences punishable by at least 180 penalty units. The judge or AAT member must have regard to the nature and extent of interference with the person's privacy, the gravity of the conduct constituting the offence, the extent to which information gathered under the warrant would be likely to assist an investigation, and other available methods of investigation.

The TIA Act contains strict prohibitions on communicating, using and making records of communications. Agencies are also required to destroy stored communications when they are no longer required for the purpose for which they were obtained.The Commonwealth Ombudsman and state oversight bodies inspect and report on agency use of interception powers to ensure law enforcement agencies exercise their authority appropriately. Agencies are required to keep comprehensive records to assist the Ombudsman and state oversight bodies for these purposes.

Additionally, agencies are required to report annually to the Minister on the:

- interceptions carried out by the agency, including
    - the use made by the agency of information obtained by interceptions
    - the communications of information to persons other than officers of the agency
    - the number of arrests made on the basis of accessed information, and
    - the usefulness of information obtained.
- stored communications accessed by agencies, including:
    - how many applications were made and warrants issued
    - the number of arrests made on the basis of the accessed information, and
    - how many court proceedings used the records in evidence.

Both the Ombudsman and Minister must table reports in Parliament each year to enable public scrutiny.

Assessment of the TIA Act

The Government keeps privacy implications and the safeguards within the TIA Act under constant review.

Although the TIA Act is not required to be subject to a human rights compatibility assessment, the Attorney-General's Department has provided extensive advice regarding the operation of the TIA Act to this committee and other Parliamentary bodies. In response to recommendation 18 of the *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* by the PJCIS in 2013, the Government agreed to comprehensively revise the TIA Act in a progressive manner. If legislation is introduced to reform the Act, the Department will undertake a human rights compatibility assessment at that time.

Foreign Influence Transparency Scheme – compatibility with the multiple rights

Committee comment

1.137 The committee therefore seeks the advice of the Attorney-General as to whether the amendments to the Foreign Influence Transparency Scheme Bill 2017 introduced by Schedule 5 pursue a legitimate objective, are rationally connected and proportionate to that objective. In particular:

- whether introducing a requirement for persons to register under the foreign influence transparency scheme when they lobby a 'political campaigner' on behalf of a foreign principal is sufficiently circumscribed, having regard to the definition of 'political campaigner' in the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017; and

- whether expanding the definition of 'political or governmental influence' to include matters raised in item 5 of schedule 5 is rationally connected to the objective of the foreign influence transparency scheme, and whether it is sufficiently circumscribed so as to constitute a proportionate limitation on human rights.

Response

Inclusion of political campaigners

The legitimate objective of the Foreign Influence Transparency Scheme (the Scheme) created by the Foreign Influence Transparency Scheme Bill (FITS Bill) is stated in the FITS Bill's Statement of Compatibility with Human Rights at paragraph 21:

> to enhance government and public knowledge of the level and extent to which foreign sources may, through intermediaries acting on their behalf, influence the conduct of Australia's elections, government and parliamentary decision-making, and the creation and implementation of laws and policies.

Extending the definition of 'general political lobbying' in section 10 of the FITS Bill to include lobbying of political campaigners registered under the *Commonwealth Electoral Act 1918* is rationally connected to the objective of the Scheme and does not unjustifiably impose limitations on human rights. The effect of the amendments is that a person or entity may be liable to register where they lobby political campaigners on behalf of a foreign principal. Whether a person is liable to register will also depend on whether the lobbying is undertaken for the purpose of political or governmental influence and whether any relevant exemptions apply.

As political campaigners occupy a significant position of influence within the Australian political system, it is appropriate that the Scheme provide transparency of the nature and extent of foreign

influence being brought to bear over such persons and entities. If not disclosed, this type of foreign influence exerted through intermediaries has the potential to impact political campaigners' positions on public policy which could, ultimately, undermine Australia's political sovereignty.

The term political campaigner is appropriately defined in order to meet the Scheme's objective while limiting its impact on human rights and cost of compliance. A political campaigner will be defined by reference to amendments to the *Commonwealth Electoral Act 1918* currently before Parliament as part of the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017 (the Electoral Funding Bill). A political campaigner will mean a person or entity that incurs 'political expenditure' during the current, or in any of the previous three, financial years of $100,000 or more. 'Political expenditure' is defined broadly as expenditure for political purposes, including, as noted by the committee, 'the public expression by any means of views on an issue that is, or is likely to be, before electors in an election.' This ensures that the range of activities undertaken by political campaigners, which may influence Australia's political and governmental processes, is captured. The financial threshold of expenditure by political campaigners imports proportionality into the Scheme and ensures it is targeted to activities most in need of transparency.

The exemptions in Division 4 of Part 2 of the FITS Bill further limit the Scheme's application in relation to political campaigners. Exemptions are provided for:

- activities undertaken to provide humanitarian aid or assistance (section 24)
- legal advice or representation (section 25)
- diplomatic, consular, United Nations and other relevant staff (section 26)
- certain religious activities (section 27)
- news media (section 28)
- commercial negotiations regarding bona fide business or commercial interests (subsection 29(1)), and
- persons employed by, or operating under the name of, the foreign principal (subsection 29(2)).

It is important to note that a requirement to register with the Scheme does not in any way preclude a person or entity from undertaking a registrable arrangement with a foreign principal, or from undertaking registrable activities on behalf of a foreign principal. This encourages and promotes the ability of decision-makers and the public to be aware of any foreign influences being brought to bear in Australia's political or governmental processes.

Definition of political or governmental influence

As noted above, a person who undertakes general political lobbying of political campaigners on behalf of a foreign principal is required to register under the Scheme where they do so for the purpose of 'political or governmental influence' and an exemption does not apply.

In order for the Scheme to meet its legitimate objective, it is necessary for the definition 'political or governmental influence' to cover the full range of processes in relation to registered political campaigners. Political campaigning is an inherently political activity, by its nature designed to influence elections, government and parliamentary decision-making, or the creation and implementation of laws and policies. It is important that the concept of 'political or governmental influence' recognises that the lobbying of political campaigners can occur in a number of ways and throughout the political cycle. A person may seek to influence the internal functioning of the political campaigner, such as its constitution, administration or membership, in order to affect the political

campaigner's external activities, including in relation to their policy position or election strategy. For example, a person acting on behalf of a foreign principal may seek to adjust a political campaigner's funding decisions as an indirect method of influencing policy priorities. The definition of 'political or governmental influence' furthers the legitimate objective of the Scheme to bring public awareness to the range of activities in need of greater transparency.

Right to Privacy

The FITS Bill requires minimal information to be provided by registrants upfront, which helps to safeguard registrants' right to privacy. The information to be collected is limited to that which is essential for the effective administration of the Scheme (see Division 2 of Part 4 of the FITS Bill - Register of scheme information), to provide decision-makers and the public with visibility of the foreign influences in Australia's political and governmental processes, and to allow for appropriate investigations into potential non-compliance with the Scheme. Only a subset of information provided will be made publicly available, further safeguarding registrants' right to privacy (see section 43).

2016-2017-2018

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

OPC drafter to complete	
1. Do any of these amendments need a message? (See H of R Practice, sixth ed, pp. 423-427, and OGC advice.) If yes: • List relevant amendments— • Prepare message advice (see DD 4.9) • Give a copy of the amendments and the message advice to the Legislation area.	No
2. Are these amendments for consideration by the Senate? If yes, go on to question 3.	No
3. Should any of these amendments be moved in the Senate as requests? (See OGC advice) If yes: • List relevant amendments— • Prepare section 53 advice and fax to relevant Ministers, the PLO in the Senate and the PLO in the House of Reps (see DD 4.9); • Give a copy of the request advice to the Legislation area with the copy of the amendments (see question 1).	No

National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

(Government)

(1) Schedule 1, item 16, page 22 (lines 9 and 10), omit subsection 90.5(1), substitute:

(1) ***Security classification*** means:

(a) a classification of secret or top secret; or

(b) any other equivalent classification or marking prescribed by the regulations.

[definition of security classification]

(2) Schedule 1, item 17, page 23 (lines 25 and 26), omit subsection 91.1(3).

[strict liability]

(3) Schedule 1, item 17, page 25 (after line 3), after paragraph 91.3(1)(a), insert:

(aa) the person deals with the information or article for the primary purpose of making the information or article available to a foreign principal or a person acting on behalf of a foreign principal; and

[primary purpose of dealing]

(4) Schedule 1, item 17, page 25 (lines 7 to 9), omit paragraph 91.3(1)(c), substitute:

(c) the information or article has a security classification.

[dealing with security classified information]

(5) Schedule 1, item 17, page 25 (lines 11 to 14), omit subsection 91.3(2), substitute:

(2) For the purposes of paragraphs (1)(aa) and (b), the person must intend the information or article to be made available to a foreign principal or a person acting on behalf of a foreign principal, even if:

(a) the person does not have in mind any particular foreign principal; or

(b) the person has in mind more than one foreign principal.

[primary purpose of dealing]

(6) Schedule 1, item 17, page 25 (line 15), omit subsection 91.3(3).

[strict liability]

(7) Schedule 1, item 17, page 26 (lines 19 and 20), omit subparagraph 91.6(1)(b)(i).

[security classification]

(8) Schedule 1, item 17, page 27 (line 4), omit subsection 91.6(3).

[strict liability]

(9) Schedule 2, item 6, page 50 (lines 1 to 6), omit paragraph (a) of the definition of ***cause harm to Australia's interests*** in subsection 121.1(1), substitute:

(a) interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth; or

[cause harm to Australia's interests]

(10) Schedule 2, item 6, page 50 (lines 22 to 25), omit paragraphs (d) and (e) of the definition of ***cause harm to Australia's interests*** in subsection 121.1(1).

[cause harm to Australia's interests]

(11) Schedule 2, item 6, page 50 (line 26), omit "the public", substitute "the Australian public".

[cause harm to Australia's interests]

(12) Schedule 2, item 6, page 50 (line 27), omit "the public", substitute "the Australian public".

[cause harm to Australia's interests]

(13) Schedule 2, item 6, page 51 (line 4), omit "contract.", substitute "contract;".

[reporting news etc.]

(14) Schedule 2, item 6, page 51 (line 4), at the end of the definition of ***Commonwealth officer*** in subsection 121.1(1), add:

; but does not include an officer or employee of, or a person engaged by, the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.

[reporting news etc.]

(15) Schedule 2, item 6, page 51 (line 5), omit "the meaning given by subsection 90.1(1)", substitute "the same meaning as in Part 5.2".

[definition of deal]

(16) Schedule 2, item 6, page 51 (after line 5), at the end of the definition of ***deal*** in subsection 121.1(1), add:

Note: For the definition of ***deal*** in that Part, see subsections 90.1(1) and (2).

[definition of deal]

(17) Schedule 2, item 6, page 51 (after line 12), after the definition of ***domestic intelligence agency*** in subsection 121.1(1), insert:

foreign military organisation means:

(a) the armed forces of the government of a foreign country; or

(b) the civilian component of:

(i) the Department of State of a foreign country; or

(ii) a government agency in a foreign country;

that is responsible for the defence of the country.

[reporting news etc.]

(18) Schedule 2, item 6, page 51 (lines 23 to 26), omit paragraph (d) of the definition of ***inherently harmful information*** in subsection 121.1(1).

[inherently harmful information]

(19) Schedule 2, item 6, page 52 (after line 2), after the definition of ***Regulatory Powers Act*** in subsection 121.1(1), insert:

security classification has the meaning given by section 90.5.

[definition of security classification]

(20) Schedule 2, item 6, page 52 (line 4), omit "(within the meaning of section 90.4)".

[definition of security classification]

(21) Schedule 2, item 6, page 53 (line 2), omit the heading to section 122.1, substitute:

122.1 Communication and other dealings with inherently harmful information by current and former Commonwealth officers etc.

[offences by current and former Commonwealth officers etc.]

(22) Schedule 2, item 6, page 53 (line 7), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(23) Schedule 2, item 6, page 53 (line 18), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(24) Schedule 2, item 6, page 54 (line 1), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(25) Schedule 2, item 6, page 54 (line 13), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(26) Schedule 2, item 6, page 54 (lines 18 and 19), omit subsection 122.1(5).

[strict liability]

(27) Schedule 2, item 6, page 54 (line 20), omit the heading to section 122.2, substitute:

122.2 Conduct by current and former Commonwealth officers etc. causing harm to Australia's interests

[offences by current and former Commonwealth officers etc.]

(28) Schedule 2, item 6, page 54 (line 29), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(29) Schedule 2, item 6, page 55 (line 13), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(30) Schedule 2, item 6, page 55 (line 31), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(31) Schedule 2, item 6, page 56 (line 13), omit "or any other".

[offences by current and former Commonwealth officers etc.]

(32) Schedule 2, item 6, page 56 (lines 24 to 26), omit subparagraph 122.3(1)(b)(i).

[security classification]

(33) Schedule 2, item 6, page 57 (line 15), omit subsection 122.3(3).

[strict liability]

(34) Schedule 2, item 6, page 57 (lines 23 and 24), omit the heading to section 122.4, substitute:

122.4 Unauthorised disclosure of information by current and former Commonwealth officers etc.

[offences by current and former Commonwealth officers etc.]

(35) Schedule 2, item 6, page 58 (after line 1), after section 122.4, insert:

122.4A Communicating and dealing with information by non-Commonwealth officers etc.

Communication of information

(1) A person commits an offence if:

(a) the person communicates information; and

(b) the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(d) any one or more of the following applies:

(i) the information has a security classification of secret or top secret;

(ii) the communication of the information damages the security or defence of Australia;

(iii) the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth;

(iv) the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

Note: For exceptions to the offences in this section, see section 122.5.

Penalty: Imprisonment for 10 years.

Other dealings with information

(2) A person commits an offence if:

(a) the person deals with information (other than by communicating it); and

(b) the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(d) any one or more of the following applies:

(i) the information has a security classification of secret or top secret;

(ii) the dealing with the information damages the security or defence of Australia;

(iii) the dealing with the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against of a law of the Commonwealth;

(iv) the dealing with the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

Penalty: Imprisonment for 3 years.

Proof of identity not required

(3) In proceedings for an offence against this section, the prosecution is not required to prove the identity of the other person referred to in paragraph (1)(c) or (2)(c).

[offences by others]

(36) Schedule 2, item 6, page 60 (lines 1 to 10), omit subsection 122.5(6), substitute:

Information dealt with or held by persons engaged in reporting news etc.

(6) It is a defence to a prosecution for an offence by a person against this Division relating to the dealing with or holding of information that:

(a) the person dealt with or held the information in the person's capacity as a person engaged in reporting news, presenting current affairs or expressing editorial content in news media; and

(b) at that time, the person reasonably believed that dealing with or holding the information was in the public interest (see subsection (7)).

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

[reporting news etc.]

(37) Schedule 2, item 6, page 60 (lines 11 and 12), omit "paragraph (6)(a), dealing with or holding information is not", substitute "paragraph (6)(b), a person may not reasonably believe that dealing with or holding information is".

[reporting news etc.]

(38) Schedule 2, item 6, page 60 (lines 25 to 27), omit paragraph 122.5(7)(d), substitute:

(d) either:

(i) in relation to an offence against subsection 122.4A(1) or (2) that applies because of subparagraph 122.4A(1)(d)(iv) or (2)(d)(iv)—dealing with or holding information that, at that time, will or is likely to result in the death of, or serious harm to, a person; or

(ii) otherwise—dealing with or holding information that, at that time, will or is likely to harm or prejudice the health or safety of the Australian public or a section of the Australian public;

[reporting news etc.]

(39) Schedule 2, item 6, page 60 (after line 27), at the end of subsection 122.5(7), add:

(e) dealing with or holding information for the purpose of directly or indirectly assisting a foreign intelligence agency or a foreign military organisation.

[reporting news etc.]

PARLIAMENT OF AUSTRALIA

Speaker of the House of Representatives *President of the Senate*

20 February 2018

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Suite R G 30
Parliament House

Dear Mr Goodenough

We refer to your letter of 7 February 2018 requesting our response in relation to the human rights compatibility of the *Parliamentary Service Amendment (Managing Recruitment Activity and Other Measures) Determination 2017* as set out in the Committee's Report 1 of 2018.

Specifically, the Committee seeks advice as to whether arrangements for publishing terminations of employment for breaching the Code of Conduct in the Public Service *Gazette* will be discontinued by the Parliamentary Service and replaced with a new secure database of relevant information that is not accessible to the general public and whether the *Parliamentary Service Determination 2013* will be amended to reflect this approach.

In December 2017 we wrote to you following receipt of advice from the Australian Public Service Commissioner about the Commissioner's decision to discontinue arrangements for publishing terminations of employment for breaching the Code of Conduct and instead establish a secure database of employment terminations not accessible to the public, with corresponding amendments to the Australian Public Service Commissioner's Directions 2016. We advised that we will work with the Commissioner in relation to the proposed database and that once the database is established we will make appropriate amendments to the Determination. In the event the database is not accessible to the Parliamentary Departments, alternative arrangements will be put in place before the Determination is amended.

We confirm for the Committee that we remain committed to working with the Commissioner on these terms and that the Department of Parliamentary Services will follow up with the Australian Public Service Commission on their progress on the proposed database and report back to the Parliamentary Administration Advisory Group at its next meeting in early March 2018.

Yours sincerely

THE HON TONY SMITH MP

SENATOR THE HON SCOTT RYAN

PARLIAMENT HOUSE · CANBERRA ACT 2600 · TEL (02) 6277 7000

PARLIAMENT OF AUSTRALIA

Speaker of the House of Representatives | *President of the Senate*

06 DEC 2017

Mr Ian Goodenough MP
Chair
Parliamentary Joint Committee on Human Rights
Suite R G 30
Parliament House

Dear Mr Goodenough

We refer to the Australian Public Service Commissioner's response to your request for advice about the compatibility of the Australian Public Service Commissioner's Directions 2016 with the right to privacy. In particular, the Committee's concerns about the publication of names of employees in the Public Service *Gazette* whose employment is terminated for breaching the Australian Public Service Code of Conduct (Code of Conduct).

We understand that in response to the Committee's concerns, the Commissioner has advised that he will cease the current notification arrangements. In its place, the Commissioner will establish a secure database of employees whose employment is terminated for breaching the Code of Conduct.

We note the Committee has recognised that similar concerns apply to Parliamentary Service employees who breach the Parliamentary Service Code of Conduct.

We will work with the Commissioner in relation to the proposed database. Once the database is established, we will make appropriate amendments to the *Parliamentary Service Determination 2013*. In the event the database is not accessible to the Parliamentary Departments, alternative arrangements will be put in place before the Determination is amended.

Yours sincerely

THE HON TONY SMITH MP

SENATOR THE HON SCOTT RYAN

PARLIAMENT HOUSE • CANBERRA 2600 • TEL (02) 6277 7111