Responses from legislation proponents — Report 7 of 2020[1]

1 This can be cited as: Parliamentary Joint Committee on Human Rights, Responses from legislation proponents, *Report 7 of 2020*; [2020] AUPJCHR 102.

The Hon Greg Hunt MP
Minister for Health
Minister Assisting the Prime Minister for the Public Service and Cabinet

Ref No: MC20-012000

Senator the Hon Sarah Henderson
Chair
Parliamentary Joint Committee on Human Rights
human.rights@aph.gov.au

28 MAY 2020

Dear Senator Sarah

Thank you for your letter of 30 April 2020 concerning the report of the Parliamentary Joint Committee on Human Rights into COVID-19 legislation (Report). The Report notes that statement of compatibility with human rights were not prepared for the measures made under the *Biosecurity Act 2015* (Cth) (Biosecurity Act) and seeks information about the interaction between those measures and human rights.

As a result of the COVID-19 pandemic, governments around the world have taken unprecedented steps to contain the outbreak. In January 2020, 'human coronavirus with pandemic potential' was listed as a human disease in the *Biosecurity (Listed Human Diseases) Determination 2016*. Since that time I have made a number of instruments to manage and respond to risks to human health caused by the pandemic.

The *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) (Human Rights Act) authorises the Committee to examine all Bills and legislative instruments for compatibility with human rights. However, as the Report acknowledges, the Human Rights Act does not require a statement of compatibility to be prepared in respect of instruments that are not disallowable legislative instruments (section 9(1)), as are the instruments that I have made to respond to the COVID-19 pandemic to date. The structure of the Biosecurity Act, and the deliberate decision by the Parliament of Australia not to make these instruments disallowable, reflects the urgency that accompanies such measures and extraordinary circumstances in which they are made.

Responding to the COVID-19 pandemic has had a significant impact on my Department, which has diverted substantial resources from other priorities to support the Government's efforts to keep Australia safe. The fact that statements of compatibility were not prepared for these instruments should not be taken to indicate that such rights are not a key consideration in the Government's response. Indeed, the measures taken have engaged a wide variety of human rights. In particular, measures taken have been in support of the right to life, as enshrined in Article 6(1) of the International Covenant on Civil and Political Rights (ICCPR), and the right to physical and mental health, as enshrined in Article 12 of the International Covenant on Economic, Social and Cultural Rights, which includes measures to prevent, treat and control epidemics.

Consistent with international law, which recognises that reasonable limits may be placed on human rights in certain circumstances, these measures do engage some human rights for the purposes of preventing or controlling the entry, emergence, establishment or spread of COVID-19. In particular, a number of measures engage the rights to liberty and freedom of movement by:

- establishing 'health response zones' to temporarily quarantine individuals returning from high risk locations, including Wuhan in China, to prevent the spread of the virus in Australia
- limiting the movement of individuals identified as high risk of transmitting the virus to prevent further spread of COVID-19
- limiting access to remote indigenous communities to protect the vulnerable populations of those areas from infection.

A number of measures also apply to identifiable groups or individuals, and engage the rights to equality and/or non-discrimination. These measures apply according to objective criteria to reduce the risk posed to or from the particular group. For example, prohibiting Australians from overseas travel reduces the risk of infection to the individual overseas and to persons in Australia on their return.

The ICCPR, the Convention on the Rights of Persons with Disabilities, and the Convention on the Rights of the Child protect the right to privacy. A number of the measures considered in the Report, as well as those made in support of the COVIDSafe App, including the emergency determination and subsequent legislation to enshrine the privacy protections into primary legislation, engage the right to privacy. The measures apply only to individuals either voluntarily providing information, seeking to travel internationally, or seeking to enter specified locations or zones. The information collected for these purposes is subject to the protections in the *Privacy Act 1988* (Cth).

I am satisfied that the measures taken by the Government are necessary and appropriate to prevent or control the entry, emergence, establishment or spread of COVID-19 in Australia and are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights Act.

Finally, I would like to assure the Committee that compatibility with human rights will continue as an important consideration in the development of any additional measures taken by the Government in addressing the COVID-19 pandemic.

Thank you for writing on this important matter.

Yours sincerely

Greg Hunt

cc: The Hon Christian Porter MP, Attorney-General and Minister for Industrial Relations

The Hon Michael McCormack MP

Deputy Prime Minister
Minister for Infrastructure, Transport and Regional Development
Leader of The Nationals
Federal Member for Riverina

Ref: MC20-003656

21 MAY 2020

Ms Sarah Henderson MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600
via human.rights@aph.gov.au

Dear Sarah Chair

Thank you for your email of 30 April 2020 regarding the issues raised in Report 5 of 2020 of the Parliamentary Joint Committee on Human Rights about the following Civil Aviation Safety Authority (CASA) COVID-19 exemption instruments:

- *CASA EX57/20 — Licensing, and Operator Training and Checking (Extensions of Time Due to COVID-19) Exemptions Instrument 2020 [F2020L00337];* and

- *CASA EX63/20 — Licensing, and Operator Training and Checking (Extensions of Time Due to COVID-19) Exemptions Amendment Instrument 2020 (No. 1) [F2020L00412].*

Your Committee was concerned that the Statements of Compatibility with Human Rights contained in the Explanatory Statements for these two instruments did not address potential issues of human rights arising under Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

I referred your Committee's concerns to CASA to consider the issues raised. I understand CASA has revised the relevant Statements of Compatibility and submitted the updated Explanatory Statements to the Federal Register of Legislation.

The Hon Michael McCormack MP
Parliament House Canberra | (02) 6277 7520 | minister.mccormack@infrastructure.gov.au
Suite 2, 11-15 Fitzmaurice Street, Wagga Wagga NSW 2650 | michael.mccormack.mp@aph.gov.au

CASA has also identified two additional related COVID-19 exemption instruments not mentioned in your correspondence but potentially giving rise to the same issue, namely:

- *CASA EX70/20 — Licensing, and Operator Training and Checking (Extensions of Time Due to COVID-19) Exemptions Amendment Instrument 2020 (No. 2)* ***[F2020L00457];*** and

- *CASA EX69/20 – EPC Requirements for ATOs Transitioning to the FER (Extensions of Time Due to COVID-19) – Exemption Amendment Instrument 2020 (No. 1)* ***[F2020L00456].***

I understand CASA has adopted the same course of action with regard to these two additional exemption instruments.

Thank you for bringing your Committee's concerns to my attention and I trust this information is of assistance.

Yours sincerely

Michael McCormack

THE HON JOSH FRYDENBERG MP
TREASURER

Ref: MS20-000907

Senator the Hon Sarah Henderson
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Senator

I am writing in response to your email of 30 April 2020 on behalf of the Parliamentary Joint Committee on Human Rights regarding the *Foreign Acquisitions and Takeovers Amendment (Threshold Test) Regulations 2020* (the 2020 Regulations). In *Report 5 of 2020: Human rights scrutiny report of COVID-19 legislation* (the Report), the Committee sought my advice as to the compatibility of the 2020 Regulations with the rights of equality and non-discrimination.

The *Foreign Acquisitions and Takeovers Act 1975* (the Act) allows the Treasurer to review foreign investment proposals that meet certain criteria. The Treasurer has the power to block foreign investment proposals or apply conditions to the way proposals are implemented to ensure they are not contrary to the national interest. The criteria that, if met, would require a proposed investment to be reviewed by the Treasurer, include whether the consideration for the proposed investment meets the monetary thresholds prescribed in the *Foreign Acquisitions and Takeovers Regulation 2015* (the 2015 Regulation). The 2020 Regulations amend the monetary threshold in the 2015 Regulation.

As the Report notes, it is the framework, which is set out in the Act, and which allows for acquisitions by foreign persons to be screened, that directly engages the rights of equality and non-discrimination. However, given the nature of the regulated activity, the extent of any incompatibility is likely to be small, and comprehensively outweighed by the national interest protected by the 2020 Regulations. As the Committee notes, this measure is designed to safeguard the national interest by protecting vulnerable businesses as COVID-19 puts intense pressure on the Australian economy and Australian businesses.

The significant impact of Coronavirus on the Australian economy has increased the risk of foreign investment in Australia occurring in ways that would be contrary to the national interest. To the extent that the 2020 Regulations engage the rights of equality and non-discrimination, limits imposed on those rights are thus reasonable, necessary and proportionate.

Yours sincerely

THE HON JOSH FRYDENBERG MP

15 / 5 /2020

Parliament House Canberra ACT 2600 Australia
Telephone: 61 2 6277 7340 | Facsimile: 61 2 6273 3420

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

Ref No: MS20-000841

Senator the Hon Sarah Henderson
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Senator Sarah,

Thank you for your letter dated 9 April 2020 requesting further information on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020.

My response for the Committee's consideration is attached.

Yours sincerely

PETER DUTTON 18/05/20

Response to Parliamentary Joint Committee on Human Rights report into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Briefly, the primary objective of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill) is to introduce a new framework for international production orders for Australia to give effect to bilateral and multilateral cross-border access to data agreements between Australia and other countries.

The Committee has raised a number of queries in relation to the Bill, especially with respect to the right to privacy and the right to an effective remedy. Please find below responses to those queries.

Committee comment 1.48: In order to fully assess the proportionality of this proposed measure, in particular the adequacy of the safeguards that apply, further information is required as to:

1. ***why the bill does not include provision for Public Interest Monitors to apply nationwide (rather than only in Victoria and Queensland) and why the Monitors have no role in an application for an IPO to access stored telecommunications data;***

In accordance with the current approach to domestic interception warrants under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the Bill aligns international production orders for interception to ensure that, where Public Interest Monitors are available in relation to domestic interception warrants, they will also be available for interception international production orders.

At present, the Public Interest Monitors only exist within Victoria and Queensland. Other Australian states and territories have not legislated for this office within their jurisdictions. Consequently, the Bill reflects this and only provides for the Public Interest Monitors in Victoria and Queensland. These authorities were established in Victoria under the *Public Interest Monitor Act 2011* (Vic), and various pieces of legislation in Queensland, including the *Police Powers and Responsibilities Act 2000* (Qld) and the *Crime and Corruption Act 2001* (Qld).

Currently, the Victorian and Queensland Public Interest Monitors perform an oversight role over their jurisdiction's law enforcement agencies including when applying for certain types of warrants, such as interception warrants. Consistent with these laws, the Bill intentionally gives the ability to facilitate the role of the Public Interest Monitors for international production orders relating to interception.

2. ***whether the interference with the right to privacy is greater for the interception of communications than accessing stored communications data, and if so, why;***

The thresholds in the Bill reflect the current thresholds for the use of similar powers under the TIA Act. The creation of a 'stored communications' framework, governing access to email, SMS, voicemail, and other stored communications held by carriers, was a recommendation of the 2005 *Review of the Regulation of Access to Communications*. This Review considered stored communications were distinct from those communications intercepted live because written communications provided an opportunity for 'second thoughts' and the potential avoidance of self-incrimination which was not possible during spontaneous communication like calls. The ability to think twice meant that access to stored communications was less privacy intrusive and could therefore occur at a lower offence threshold than telecommunications interception. (Anthony Blunn, *Review of the Regulation of Access to Communications* (2005) paras 1.4.2-1.4.3).

The terms of reference for the Comprehensive Review of the Legal Framework of the National Intelligence Community (the Comprehensive Review) included reviewing legislation containing

agency investigative powers, such as the *Surveillance Devices Act 2004* and the TIA Act. The Government will consider the findings of the Comprehensive Review.

3. ***why the power to issue an IPO is conferred on a member of the AAT, of any level and with a minimum of five years' experience as an enrolled legal practitioner, and whether this is consistent with the international human rights law requirement that judicial authorities issue surveillance warrants;***

The Bill provides for a range of independent decision-makers to authorise interception activities, and access to stored communications and telecommunications data. A comparison table for the Committee's convenience breaking down which decision-makers can authorise different types of international production orders and the current TIA Act warrants and authorisations is at **Annexure A**.

The role of nominated Administrative Appeals Tribunal (AAT) members is critical as independent decision makers in authorising investigatory powers under the TIA Act. This is alongside judges (and magistrates in certain instances).

For example, nominated AAT members have played a role in approving interception warrants under the TIA Act since 1998. The role of nominated AAT members as independent issuing authorities also exists in other legislation, such as the *Surveillance Devices Act 2004*.

For national security international production orders, the involvement of the Attorney-General reflects the current issuing process for domestic national security orders for interception and access to stored communications, which also require ministerial authorisation.

While it is important to ensure that there is a lawful and independent decision-maker in investigatory powers legislation, there is no requirement under international human rights law for Australia to ensure specifically that it is a judicial authority that authorises investigatory powers. This position is reflected in other legislation including the *Surveillance Devices Act 2004* and the TIA Act.

4. ***why does the bill not require, in all instances, that before issuing an IPO the decision maker turn their mind to considering whether doing so would be likely to have the least interference with a person's privacy;***

The privacy considerations that must be taken into account are tailored to the international production order being sought. When considering an application for an interception international production order in relation to a control order under Part 3 of Schedule 1 to the Bill, the decision maker must consider whether interception would be the method that is likely to have the least interference with any person's privacy. This additional protection is considered appropriate because control order international production orders have a protective or preventative purpose by facilitating monitoring of the person's compliance with the requirements of the control order, and the person is not necessarily suspected of involvement in further criminal activity since the control order was imposed.

While this requirement does not apply to international production orders for law enforcement and national security, authorities considering applications for those orders will be required to have regard to privacy impacts in deciding whether to issue those orders. For example, for international production orders under Part 2 of the proposed Schedule, before issuing an international production order for law enforcement, the decision maker must consider, among other things,

- how much the privacy of any person or persons would be likely to be interfered with by intercepting communications;
- the gravity of the alleged conduct;

- to what extent methods of investigating the [serious offences] that do not involve intercepting communications have been used by, or are available to, the interception agency;
- how much the use of such methods would be likely to assist in connection with the investigation by the interception agency of the [serious offences]; and
- how much the use of such methods would be likely to prejudice the investigation, whether because of delay or for any other reason.

The decision maker for an international production order for national security must consider, among other things:

- to what extent methods of obtaining intelligence relating to security that are less intrusive have been used by, or are available to the Australian Security Intelligence Organisation (ASIO);
- how much the use of such methods would be likely to assist ASIO in obtaining intelligence relating to security; and
- how much the use of such methods would be likely to prejudice ASIO in carrying out its function of obtaining intelligence relating to security.

Taken in totality, these considerations ensure that the decision maker conducts a thorough assessment of the privacy impacts of the order, and that actions taken under the international production, including the necessary interference with a person's privacy, are proportionate to the relevant conduct.

In addition, ASIO is subject to separate requirements for conducting its activities, including under *'Ministerial Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluation and communicating intelligence relevant to security (including politically motivated violence)'*, issued under section 8A of the *Australian Security and Intelligence Organisation Act 1979*.

The Guidelines provide that information to be obtained by ASIO is to be done in a lawful, timely and efficient way and in accordance with the following:

- any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence;
- inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions; and
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

B-Party considerations for interception international production orders

B-Party interception assists law enforcement agencies and ASIO to counter measures adopted by persons of interest to evade electronic surveillance, such as adopting multiple telecommunications services. The ability, as a last resort, to target the communications of an associate of a person of interest will ensure that the utility of interception is not undermined by evasive techniques adopted by persons of interest.

B-Party interception may only be authorised for a period of 45 days, a shorter period than applicable to non B-Party interception (90 days), acknowledging this type of interception inherently involves greater privacy intrusion.

Additionally, the decision-maker is further restricted from issuing a B-Party interception international production order unless they are satisfied the agency has exhausted all other practicable methods of identifying the services that is being used by the person alleged to be committing the serious crimes.

In the case of national security international production orders, the nominated AAT Security Division member must consider whether other, less intrusive means of obtaining intelligence relating to security are available, or have been used, which must be weighed against its effectiveness and potential to prejudice ASIO in carrying out its functions.

5. why the bill does not require, in all instances, that IPOs may only be issued where to do so will be likely to 'substantially' assist an investigation (rather than simply being 'likely to assist');

The thresholds adopted for the Bill broadly mirror existing domestic warrant thresholds.

The decision to use the terminology *'likely to assist'* as opposed to *'substantially assist'* was made to provide Australia's national security and law enforcement agencies with the operational flexibility they need to carry out their functions in order to investigate, detect and prevent serious crimes, and threats to national security including terrorism. For example, telecommunications data, such as account details and IP addresses, are often collected during the early stages of an investigation. When seeking an order, agencies need to demonstrate that this information is likely to assist the investigation, for example by determining a link between an account and the suspected criminal activity or offender and thereby identifying further lines of inquiry. As well as this, it would be reasonably appropriate for the requesting agency to establish that the disclosure of the relevant information would be likely to assist in connection with the investigation. However, particularly during the early stages of an investigation, it would be extremely difficult for agencies to demonstrate in advance of reviewing the information that the information would 'substantially assist' the investigation.

Control order international production orders have a higher threshold of 'substantially assist'. As noted in the response to question 4, the Government considers it appropriate for additional protections in relation to control order international production orders. This is because these orders have a protective or preventative purpose. The use of 'substantially assist' also reflects the threshold for domestic interception warrants in relation to control orders under the TIA Act, and the grounds for issuing a control order under Division 104 of the *Criminal Code Act 1995*. These include, amongst other grounds, that the control order would 'substantially assist' in preventing a terrorist act or provision of support for or facilitation of a terrorist act

6. how the timeframe for the duration of an interception IPO was chosen and why interception IPOs issued in connection with carrying out ASIO's functions are twice as long as those to investigate serious offences;

The maximum duration for interception international production orders aligns with the requirements of the TIA Act. Under section 9B(3A) of the TIA Act, ASIO interception warrants must not exceed 6 months (or 3 months in the case of B-party warrants). Under section 49(3) of the TIA Act, law enforcement interception warrants must not exceed 90 days (or 45 days for B-party warrants). In cases where interception is required, longer timeframes are necessary to support operational requirements. As these operations are often highly changeable, this means that the orders that support them require a higher degree of flexibility. For this reason, interception orders have a longer maximum timeframe than other orders.

The nature of ASIO's work is primarily focused on the prevention and detection of activities prejudicial to security. As a result, timeframes often shift and the threat level is constantly changing.

ASIO's focus on the identification, prevention and disruption of security threats requires a longer-term view of activities, involving the recruitment or radicalisation phases (of either espionage or politically motivated violence activities), as well as the planning and operational phases. This means that these are often protracted investigations, necessitating the ability to apply for an international production order of longer duration.

The Bill also requires the issuing authority to consider specific factors in determining whether to issue an international production order and the issuing authority can also consider any other matters it considers relevant. One of these other relevant matters may be the duration of the order and the Bill provides sufficient flexibility for issuing authorities to determine a shorter period of duration for an order in appropriate circumstances.

In practice, the duration of an interception international production order would be determined on a case-by-case basis by the decision-maker determining the application. The period of time sought for interception activities would be determined by the requirements of each individual investigation, and the agency applying for the order would be responsible for furnishing the decision-maker with sufficient evidence to justify the appropriate duration for interception under the order.

7. ***why there is no provision in the bill to ensure that if the circumstances that led to the issuing of the IPO have changed, such that the IPO is no longer warranted, that the IPO ceases to have effect;***

Clauses 114 and 116 of Schedule 1 to the Bill place an obligation on the chief officer of agencies and the Director-General of Security to revoke an order if satisfied that the grounds on which the order was issued have ceased to exist. The revocation must be set out in a written instrument. In circumstances where an order is revoked after it has been given to the designated communications provider, clauses 115 and 117 place an obligation on the agency to give the instrument of revocation to the Australian Designated Authority. The Australian Designated Authority would then have an obligation to give the instrument to the designated communications provider as soon as practicable.

This mechanism is designed to remove any doubt about the status of an international production order when the grounds for issuing an order no longer exist and the time at which the order ceased to be in force. It will also serve to protect privacy by clearly indicating to the agency, the Australian Designated Authority and the designated communications provider, that the order has ceased to be in force.

8. ***why are existing powers to investigate serious crimes insufficient to achieve the objectives of the measure, such that a separate power to issue an IPO in relation to control orders is considered necessary;***

Terrorism poses a significant threat to national security and public safety, and is of substantial concern for law enforcement agencies and the Australian community. The control order regime addresses the challenge posed by terrorism or by involvement in hostile activity in a foreign country by mitigating the threat posed by specific, high-risk individuals. The use of interception warrants under the TIA Act to monitor those subject to control orders supports the monitoring of compliance with conditions imposed, and better mitigates the risk of terrorism and involvement in hostile activity in a foreign country. If a person subject to a control order perceives there is little likelihood of non-compliance with the control order being detected, there is little incentive for them to comply with the terms of the order, and the specific preventative effect of a control order is potentially undermined.

Under the existing TIA Act, agencies are able to obtain domestic warrants and authorisations for data held by Australian communications service providers for the purposes of monitoring a person subject to a control order, and to detect planning and preparatory acts for a terrorist act or in hostile activity in a foreign country. However, these powers are increasingly unlikely to be effective in all cases due to Australians' increasing use of online communications platforms operated from foreign countries and data stored internationally, outside of Australian agencies' reach.

Accordingly, the Government considers it appropriate to enable certain agencies to apply for control order international production orders in order to obtain information from designated communications providers based overseas that are covered by a designated international agreement. Consistent with

the TIA Act framework for domestic warrants in relation to control orders, agencies will only be able to apply for control order international production where the relevant thresholds can be met.

9. why do the control order IPOs not require the judge or AAT member to consider the gravity of the conduct being investigated;

Control order international production orders would be issued for the purposes of protecting the public from terrorist acts, preventing the provision of support for terrorist acts or involvement in hostile activity in a foreign country, or to determine whether a control order is being complied with. As control order international production orders have a protective or preventative purpose, the person to be targeted would not necessarily be suspected of any specific criminal conduct. Given this, the Government considers that the gravity of the conduct being investigated does not need to be a mandatory consideration for control order international production orders.

10. what does conduct that is 'prejudicial to security' mean, and is this sufficiently certain to allow people to know what conduct it covers;

The Bill enables ASIO to seek international production order on the basis of thresholds which are also utilised in many of ASIOs warrants and which, in most cases (in relation to orders for interception or stored communications), centre on the concept of a person engaged in, or reasonably suspected of being engaged in, or being likely to engage in, *activities prejudicial to security.*

The phrase *'activities prejudicial to security'* is not exhaustively defined in the ASIO Act or the TIA Act. Section 4 of the ASIO Act provides that *'activities prejudicial to security'* includes any activities concerning which Australia has responsibilities to a foreign country as referred to in paragraph (b) of the definition of security in this section. Section 4 of the ASIO Act defines ***security*** as meaning:

> (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
>
> (i) espionage;
>
> (ii) sabotage;
>
> (iii) politically motivated violence;
>
> (iv) promotion of communal violence;
>
> (v) attacks on Australia's defence system; or
>
> (vi) acts of foreign interference;
>
> whether directed from, or committed within, Australia or not; and
>
> (aa) the protection of Australia's territorial and border integrity from serious threats; and
>
> (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

The terms '*Acts of foreign interference*' '*attacks on Australia's defence*' *'politically motivated violence*' and '*promotion of communal violence'* are each further defined in the ASIO Act.

Conduct that is prejudicial to security would therefore cover a person's engagement in any of the above activities, including planning the activities. For example, a person would be engaged in conduct that is prejudicial to security if the person engages in espionage or plans a terrorist attack.

This term is used across a range of Acts and other instruments relating to Australian national security. In particular, the TIA Act adopts the term in the threshold for domestic interception warrants for ASIO. The ASIO Act adopts the term in the thresholds for surveillance device warrants and identified person warrants.

The Ministerial Guidelines to which ASIO is subject provide that *activities relevant to security* not only means physical acts of the sort specified in the definition of security but also includes the acts of conspiring, planning, organising, counselling, advising, financing, or otherwise advocating or encouraging the doing of those things. The Guidelines also provide that *activities prejudicial to security* means activities that are relevant to security and which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities.

11. why can an IPO to access telecommunications data be granted if it would be in connection with the performance of ASIO's functions, without any other requirement that there is any alleged prejudice to national security;

The threshold 'in connection with the performance of ASIO of its functions' reflects the threshold in the TIA Act. The decision to use this threshold was made to provide ASIO with the operational flexibility it needs to carry out its functions. International production orders for interception and stored communications have an additional requirement that there are reasonable grounds for suspecting the person is engaged in, or is likely to engage in, activities prejudicial to security. The Government considers it appropriate for additional protections to apply to international production orders for interception and stored communications.

Under section 8A of the ASIO Act, ASIO is required to comply with Ministerial Guidelines. These guidelines stipulate that when conducting its activities, ASIO must apply the principle of proportionality to ensure the least intrusion necessary into an individual's privacy, and any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence. Therefore whilst clause 107 only requires that the international production order be in connection with the performance of ASIO's functions, in practice the decision to seek access to telecommunications data must only be made in circumstances where the decision-maker is satisfied that the disclosure is in connection with the performance by ASIO of its functions, is proportionate to the gravity of the threat posed and the probability of its occurrence, and will be undertaken with as little intrusion into individual privacy as possible.

Access to telecommunications data enables preliminary investigative work to be undertaken that can rule individuals in or out of further investigation. Without telecommunications data, other potentially more intrusive investigative methods would need to be employed in order to make the appropriate assessment that an individual meets the required threshold for investigation. Alternatively, without telecommunications data, an investigation may not be undertaken due to lack of information to establish the required threshold (for example, to meet the threshold for international production order for telecommunications interception or stored communications), potentially increasing the risk of unmitigated security threats. The proposed threshold for international production order relating to telecommunications data will enable ASIO to access telecommunications data at an appropriate speed for these preliminary investigations.

12. why does the bill not provide that an AAT member when determining whether to issue an IPO must consider how much the privacy of any person would be likely to be interfered with by issuing the order, or the gravity of the conduct being investigated; and

For international production order relating to national security, the AAT member must have regard to a number of matters listed in clause 89(5), including to what extent less intrusive methods (of obtaining the information are available to ASIO, how much the use of such methods would be likely

to assist ASIO in carrying out its function of obtaining intelligence relevant to security, as well as such other matters (if any) that the nominated AAT member considers relevant. The AAT member must consider the availability of less intrusive methods and weigh such methods against how this would be likely to assist or prejudice ASIO—for example, because of delay or for other reasons.

The Bill thereby provides a broad discretion to enable the decision-maker to consider and balance the proportionality of the investigative method applied against privacy impacts and the gravity of the conduct being investigated. In this way, the Bill recognises ASIO's role as being anticipatory and protective in nature, with ASIO expected to identify and act against threats before harm has occurred. On that basis, the matters which the AAT member is required to consider are appropriate.

Further, section 10.4 of the Ministerial Guidelines to which ASIO is subject (issued under section 8A of the ASIO Act) requires ASIO to apply proportionate investigative methods, balancing the gravity of the threat posed and the probability of its occurrence.

As per our response to question 4, similar to the framework for domestic warrants under the TIA Act, authorities considering applications for international production orders would be required to make an overall assessment weighing up privacy impacts against the needs of law enforcement or national security. However, as interception of communications is considered to be the most intrusive of surveillance powers, additional requirements have been expressly included in relation to interception international production orders.

13. ***Whether all of the exceptions to the prohibition on the use, recording or disclosure of protected information obtained pursuant to an IPO are appropriate. It would be useful if a justification were provided in relation to each of the exceptions in proposed sections 153-159 and how these are compatible with the right to privacy.***

An explanation of the justification for each of the exceptions in clauses 153-159 of Schedule 1 of the Bill is set out below:

- Sub-clauses 153(1)(a), (b), (c), (d), (e) and (f): these exceptions support the objectives of protecting national security and public safety and addressing crime and terrorism by enabling agencies to deal with the information and evidence they need to investigate or prosecute serious criminal offences. The gravity of the offences and actions covered by these provisions, and potential significant impact on the Australian community should a person carry out an action means it is appropriate to limit a person's right to privacy under these exceptions.
- Sub-clause 153(1)(h): this exception supports the objective of protecting national security by enabling ASIO to access and deal with the information it needs to perform its national security functions. The objective of protecting Australia's national security illustrates an appropriate limitation on a person's right to privacy under this exception.
- Sub-clauses 153(1)(i), 153(1)(j) and 153(1)(k): these exceptions support the objectives of preventing and investigating terrorism by enabling agencies and courts to deal with the information they need to consider the issues relating to control orders, preventative detention orders and continuing detention orders. These exceptions, which aim to prevent and investigate terrorism offences, also represent a reasonable limitation on a person's right to privacy.
- Sub-clauses 153(1)(l) and (t): these exceptions ensure the effectiveness of the civil penalty regime within the Schedule. They will enable protected information to be used in investigating contraventions of the compliance provisions, such as those under Part 8, or the reporting of the outcome of those proceedings. This enhances the accountability and transparency of the regime.

- Sub-clauses 153(1)(m), (n), (o), (p), (q), (r), (3) and (4) and clauses 154 and 155: these exceptions support accountability, transparency and oversight mechanisms in proposed Schedule 1 of the TIA Act and existing legislation by enabling oversight bodies and Ministers to access the information they need to provide oversight of agencies' use of the legislation and compliance with legislative requirements. Again, the aim of ensuring appropriate oversight and accountability under these exceptions also demonstrates a reasonable limitation on a person's right to privacy.
- Sub-clauses 153(1)(u). (v), (w), (x), (y), (5), (6) and (7): these exceptions support the objectives of protecting national security and public safety and addressing crime and terrorism by enabling disclosure of information to foreign partner countries and international bodies to support investigation and prosecution of serious criminal offences. As these exceptions aim to protect Australia's national security and ensure public safety, they are also illustrating a reasonable limitation on a person's right to privacy.
- Sub-clauses 153(1)(s) and (z): these exceptions support the objective of addressing serious crime by enabling relevant stakeholders, including the Australian Designated Authority and Department of Home Affairs and law enforcement and national security agencies to deal to information necessary to administer Schedule 1 of the Bill and the designated international agreements underpinning Schedule 1 of the Bill. The gravity of the offences and actions covered by these provisions, and potential significant impact on the Australian community should a person carry out an action means it is appropriate to limit a person's right to privacy under these exceptions.
- Clause 156: this exception supports corporate transparency by enabling designated communications providers to disclose statistics to their shareholders and the public on the number of international production orders they have received. This exception balances individual privacy by only permitting the disclosure of aggregate statistics, and also go towards the aim of providing transparency and accountability.
- Clause 157: these exceptions support accountability, transparency and oversight mechanisms under Commonwealth, state and territory laws by enabling investigators, legal advisors and courts to obtain the information they need to conduct a range of legal proceedings related to integrity and anti-corruption. The aim of ensuring appropriate oversight and accountability under these exceptions also demonstrates a reasonable limitation on a person's right to privacy.
- Clause 158: these exceptions support the objectives of protecting public safety and addressing crime by enabling stored communications data obtained under an international production order to be used in a range of Commonwealth, state and territory proceedings including, for example, confiscation or forfeiture of property proceedings and coroner's inquests. Stored communications data can be invaluable to these types of proceedings and ensure the decision-maker has all the information to make fulsome decisions. These are reasonable limitations on a person's privacy to protect the safety of the community and also to support existing criminal proceedings.
- Clause 159: these exceptions support the objectives of protecting public safety and addressing crime by enabling telecommunications data obtained under an international production order to be used for purposes in connection with enforcement of a criminal law or law imposing pecuniary penalty of the protection of the public revenue. These exceptions ensure that telecommunications data that has been obtained can be used for a range of purposes to protect the community from suspected criminal conduct, misconduct and anti-competitive behaviour, in addition to assisting in the location of missing persons. The exception permits the use of telecommunications data to ensure that members of the community are meeting their lawful obligations under Australian revenue laws, such as taxation laws, in order to protect the

public revenue. These are reasonable limitations on a person's privacy to protect the safety of the community and also to support existing criminal proceedings.

Committee comment 1.53: In order to assess whether any person whose right to privacy might be violated by the issuance of an IPO would have access to an effective remedy, further information is required as to:

1. ***whether a person who was the subject of an IPO will be made aware of that after the investigation has been completed; and***

Ordinarily, persons of interest or those who were subject to covert investigatory powers are not notified of the use of covert investigatory powers unless there is a specific requirement under law to do so (for example, a prosecutor's legal obligation to disclose material used to build a case against an individual for prosecution). This has been the consistent practice for warrants under the TIA Act and other Commonwealth legislation that confers covert investigatory powers.

If a person becomes aware of the use of covert investigatory powers while the investigation is ongoing, this could obviously put the investigation at risk by tipping off those engaging in criminal conduct about the investigation and the capabilities and methodologies being employed. However, notifying a person after the conclusion of an investigation can also have significant ramifications for future law enforcement and ASIO methodologies and the legitimate need to keep technical capabilities that relate to electronic platforms/services confidential.

Public disclosure of the details of an international production order or the information collected under it may reveal to criminal entities and organisations that using that particular service is subject to, or could be subject to, electronic surveillance. For example, knowing that a certain website or forum is monitored may mean that many months or years of law enforcement efforts to penetrate crime networks (such as online child sexual abuse groups) can be lost. This ultimately reduces the effectiveness of Australian law enforcement agencies and ASIO to keep the Australian community safe from serious crime.

Even where the subject of the international production order has been cleared of any criminal activity, this does not necessarily reduce the risk that the disclosure may impact future law enforcement and ASIO methodologies and the protection of technical capabilities. For example, the person subject to the international production order could inadvertently jeopardise future law enforcement and ASIO operations by publicly announcing they were subject to certain types of orders on certain services.

While the Government acknowledges that the use of an international production order will impact a person's privacy, the Government's view is that this limitation on privacy is reasonable, necessary and proportionate in order to safeguard the Australian community from serious crime. These measures are balanced with strict safeguards, such as prohibitions on the disclosure of information obtained under a warrant excepted in limited circumstances destruction requirements, and agencies being subject to significant oversight and reporting requirements on their use of regimes. In particular, the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security pay close attention to Australian law enforcement agencies' and ASIO's respective use of covert investigatory powers.

2. ***if not, how such a person would effectively access a remedy for any violation of their right to privacy.***

Although a person would not be notified that data relating to them has been obtained under an international production order, stringent measures are in place to protect individual privacy. In keeping with the approach in the TIA Act, subject to limited exceptions, the Bill prohibits the disclosure of information obtained under an international production order, or in relation to an

international production order, in order to promote the privacy of individuals and to protect sensitive law enforcement and national security investigations.

The Bill balances the impact on privacy and the covert nature of the investigatory powers by ensuring effective oversight, record keeping, and independent authorisation. In particular, there is public ministerial reporting on the use of the regime. The Commonwealth Ombudsman and Inspector-General of Intelligence and Security will provide oversight over agencies' use of the international production order framework through audit and inspections to determine compliance with legislative requirements.

A person who is the subject of an international production order, as revealed during the preparation for or conduct of criminal proceedings, can challenge such an order and the admissibility of evidence gathered in Australian courts where evidence is used in a prosecution.

Committee comment 1.66: In order to fully assess the compatibility of the measure with the right to life and the prohibition on torture, cruel, inhuman or other degrading treatment or punishment, further information is required as to:

1. ***why the bill does not provide that an international agreement will not be designated unless there is a written assurance that information provided pursuant to an IPO will not be used in connection with any proceeding by way of a prosecution for an offence against the law of the foreign country that is punishable by death;***

The Bill requires that prior to entering into an agreement, the government of a foreign country must give the Minister written assurance about the use or non-use of Australian-sourced information in any prosecution for an offence that is punishable by death.

This provision is designed to be flexible as to the form, content and nature of the written assurance as this will depend on the particular foreign country, including their laws and practices in relation to death penalty matters, and the particular agreement, including its scope and whether it is bilateral or multilateral. It also accommodates the use of exculpatory material (material that goes towards a person's innocence) in a prosecution.

The Government anticipates that agreements will be treaties rather than instruments of less than treaty status. Parliamentary processes that precede the ratification of any agreements with foreign countries will provide checks and balances for all elements of that agreement, including ensuring Australia's opposition to the death penalty is upheld appropriately.

2. ***what safeguards are in place to ensure that information from an IPO would not be shared overseas in circumstances that could expose a person to torture, or cruel, inhuman or degrading treatment or punishment.***

Article 7 of the ICCPR states:

No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation.

Article 3(1) of the CAT states:

No State Party shall expel, return ("refouler") or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture.

While the Bill will give effect to future bilateral and multilateral cross-border access to data agreements between Australia and other countries, it does not, however, affect the substance of Australia's adherence to the prohibition against torture, cruel, inhuman or degrading treatment or punishment.

Sub-clauses 153(5), (6) and (7) of the Bill ensure that information obtained pursuant to an international production order can be provided to foreign countries in response to a mutual legal assistance (MLA) request from a foreign country and to international bodies such as the International Criminal Court and International War Crimes Tribunal. The *Mutual Assistance in Criminal Matters Act 1987* (MACMA) provides that the Attorney-General must refuse a MLA request from a foreign country where there are substantial grounds for believing that, if the request was granted, a person would be in danger of being subjected to torture (paragraph 8(1)(ca)). In instances where providing MLA to a foreign country may expose a person to other cruel, inhuman or degrading treatment or punishment, the Attorney-General has a general discretion to refuse the MLA request (paragraph 8(2)(g) of the MACMA).

This matter will be considered further in negotiations for each designated international agreement. Parliamentary processes that precede the ratification of any formal agreements with foreign countries will provide the opportunity for close scrutiny of all elements of each agreement.

Committee comment 1.72: In order to more fully assess the compatibility of this measure with the right to privacy, further information is required as to:

1. ***what is the legitimate objective of removing existing privacy protections to allow personal telecommunications data to be intercepted and accessed by foreign governments;***

Our collective safety and security depends on the ability of Australian agencies to maintain lawful and efficient access to electronic evidence. The Bill creates a framework for ensuring that Australia can enter into international cross-border access to data agreements with trusted foreign countries while respecting privacy interests and foreign sovereignty. However, the benefits of allowing Australian law enforcement agencies and ASIO to be able to directly issue orders on foreign providers, cross-border arrangements and agreements would need to be reciprocal.

For example, in order for Australia to be a qualifying foreign government that is able to enter into an agreement under the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act, it must ensure the removal of blocking statutes. Blocking statutes are laws that would prevent the United States Government from issuing legal process directly on Australian providers to access electronic information held in Australia. This means the relevant provisions under the TIA Act, *Telecommunications Act 1997,* and *Privacy Act 1988* that prevent such access must be lifted, ensuring that United States law enforcement can lawfully request this kind of information from Australian providers directly.

As transnational, serious and organised crime is becoming more prevalent, enabling reciprocal access to data will assist Australia's international partners to successfully prevent, investigate and prosecute serious criminal activity in their own jurisdictions, which can have benefits for Australia's own law enforcement efforts. Agreements negotiated will have a range of safeguards and restrictions to ensure respect for privacy and civil liberties, requirements for appropriate thresholds, and independent authorisation processes, to ensure orders are reasonable, necessary and proportionate.

2. ***what safeguards apply before foreign governments can issue an order or make such a request and what oversight mechanisms are there before such agreements are entered into.***

The overarching designated international agreement and the law of the foreign country that applies to any incoming international production order request will establish the limitations and safeguards that apply when the relevant foreign government sends orders to Australian providers, similar to the safeguards for requests made under the *Mutual Legal Assistance in Criminal Matters 1987.*

The Australian Government will undertake a thorough assessment of the privacy regime of the foreign country before entering into any agreement. Agreements will also provide for privacy matters such as the limitation on use and handling of Australian data and destruction of records.

Prior to entering into an agreement with a foreign country that applies the death penalty, the government of the foreign country must give the Minister written assurance about how Australian-sourced information will be used in any proceeding by way of prosecution for an offence that is punishable by death in the foreign country, including for exculpatory purposes. The written agreement may specify restrictions or conditions on the use of Australian-sourced information including that it is not to be used in prosecutions for death penalty offences.

The Bill also enables a foreign designated communications provider to object to an Australian international production order, because it does not comply with the designated international agreement. The Australian Designated Authority may cancel an international production order, including following dispute resolution with the designated communications provider or the government of a foreign country.

Supporting this framework will be Agreements that have a range of safeguards and restrictions to ensure respect for privacy and civil liberties, requirements for appropriate thresholds, and independent authorisation processes, to ensure orders are reasonable, necessary and proportionate.

Oversight mechanisms

Before any agreement becomes operational, the following mechanisms will assist Australia to ensure privacy protections are appropriate:

- The Australian Government will do a thorough assessment of the privacy regime of the foreign country before entering into, and during, any agreement negotiations
- The Attorney-General and the Minister for Foreign Affairs will approve any proposed agreement before it is signed. Both Ministers have unique responsibilities for both domestic and international privacy matters.
- Any agreement will be referred to the Joint Standing Committee on Treaties (JSCOT) for consideration. The Department of Home Affairs will prepare a National Interest Analysis when referring the matter to JSCOT, which will consider privacy implications.
- Stakeholders and members of the public will be able to make submissions to JSCOT indicating any privacy concerns that JSCOT will take into account before providing its recommendations.
- Before Australia can ratify an Agreement, regulations will be made under the TIA Act to declare the agreement as a 'designated international agreement'. Such regulations will be subject to the normal disallowance periods in parliament. Any disallowable legislative instruments will also be accompanied by a Statement of Compatibility with Human Rights.

Annexure A –Comparison table: Authorising authorities under the international production order framework and the domestic TIA Act framework

International production order authorising authorities			
	Law enforcement orders	**National Security orders**	**Control Order IPOs**
Interception international production order	Under clause 30, may be issued by eligible judges (clause 14) and nominated AAT members (clause 15)	Under clause 89, nominated AAT Security Division member (clause 17) (ASIO must first seek consent of the Commonwealth Attorney-General to make the application)	Under clause 60, may be issued by eligible judges (clause 14) and nominated AAT members (clause 15)
Access to stored communications international production order	Under clause 39, may be issued by issuing authorities (clause 16) (this includes magistrates, judges and certain AAT members)	Under clause 98,nominated AAT Security Division member (clause 17) (ASIO must first seek consent of the Commonwealth Attorney-General to make the application)	Under clause 69, may be issued by issuing authorities (clause 16) (this includes magistrates, judges and certain AAT members)
Access to telecommunications data international production order	Under clause 48, may be issued by issuing authorities (clause 16)	Under clause 107, nominated AAT Security Division member (clause 17)	Under clause 78, may be issued by issuing authorities (clause 16)

Current TIA Act authorising authorities			
	Law enforcement warrants	**National Security warrants**	**Control order warrants**
Interception warrants	Eligible Judges (section 6D) and nominated AAT members (section 6DA)	The Commonwealth Attorney-General (section 9)	Eligible Judges (section 6D) and nominated AAT members (section 6DA)
Access to stored communications warrant	Issuing authorities (section 6DB) (this includes magistrates, judges and certain AAT members)	N/A – access to stored communications currently granted under an interception warrant under section 9	Issuing authorities (section 6DB) (this includes magistrates, judges and certain AAT members)
Access to telecommunications data authorisation	Authorised officers of enforcement agencies (section 5AB) (this includes management offices or management positions of	Eligible person (sections 175 and 176) (this includes the Director-General of Security, the Deputy Director-General of Security and ASIO	No specific data authorisation for control orders

Current TIA Act authorising authorities			
	an enforcement agency or authorised senior executive member of the AFP, as authorised by the head of an enforcement agency or AFP Commissioner)	employees or ASIO affiliates who covered by a relevant approval from the Director-General)	