Ministerial responses — Report 3 of 2021[1]

1 This can be cited as: Parliamentary Joint Committee on Human Rights, Ministerial responses, *Report 3 of 2021*; [2021] AUPJCHR 33.

THE HON ALEX HAWKE MP
MINISTER FOR IMMIGRATION, CITIZENSHIP, MIGRANT SERVICES AND MULTICULTURAL AFFAIRS

MS21-000232

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

Dear Senator

Thank you for your correspondence of 4 February 2021 requesting advice on the Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020 (the Bill).

The Australian Government introduced the Bill to enhance the Government's ability to uphold the safety and good order of the Australian community.

The Bill amends the *Migration Act 1958* and the *Australian Citizenship Act 2007* to create a framework for the protection of information provided in confidence by gazetted law enforcement and intelligence agencies and used in character-related visa and citizenship decisions, which includes applications to revoke or set aside such decisions. Criminal intelligence and related information are vital to assess the criminal background or associations of non-citizen visa applicants and visa holders.

In the Parliamentary Joint Committee Human Rights Report 1 of 2021, the Committee sought clarification on the following matters:

- natural justice
- adequacy of judicial and merits review
- fairness to the applicant
- significant matters in delegated legislation

A copy of the detailed response is enclosed.

Thank you for raising this matter.

Yours sincerely

ALEX HAWKE

Annex A

Parliamentary Joint Committee on Human Rights, Report 1 of 2021

Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020

Minister's Response

- **why it is necessary and appropriate to use 'public interest' as opposed to 'national security' as the threshold concept for determining whether confidential information can be disclosed to another person, and a rationale for the inclusion of each of the grounds in proposed subsections 52C(5) and 503C(5);**

The measures in the Bill are necessary to strengthen the Government's ability to uphold public safety and the good order of the Australian community through character-related decisions made under both the *Migration Act 1958* (the Migration Act) and the *Australian Citizenship Act 2007* (the Citizenship Act).

The Department relies on confidential information provided by law enforcement and intelligence agencies to assess the character of visa applicants and visa holders. If the person fails the character test, they may be refused a visa, or if they hold a visa, it can be cancelled.

The changes will strengthen the framework for the protection and use of confidential information in the Citizenship Act in substantially the same way as that in the Migration Act, allowing the Department to rely on confidential information provided by law enforcement and intelligence agencies to assess the character of certain citizenship applicants, or persons whose citizenship may be considered for revocation.

Under the proposed amendments, after considering the information and any submissions, the High Court, the Federal Court of Australia, or the Federal Circuit Court (the courts) must determine if disclosure of information would create a real risk of damage to the 'public interest', having regard to any of the following matters (and only those matters) that it considers relevant. As per 52C(5) of the Citizenship Act and 503C(5) of the Migration Act, these are:

- the fact that the information was communicated, or originally communicated, to an authorised Commonwealth officer by a gazetted agency on the condition that it be treated as confidential information;
- the risk that the disclosure of information may discourage gazetted agencies and informants from giving information in the future;
- Australia's relations with other countries;
- the need to avoid disruption to national and international efforts relating to law enforcement, criminal intelligence, criminal investigation and security intelligence;
- in a case where the information was derived from an informant - the protection and safety of informants and of persons associated with informants;
- the protection of the technologies and methods used (whether in or out of Australia) to collect, analyse, secure or otherwise deal with, criminal intelligence or security intelligence; and
- such other matters (if any) as are specified in the regulations.

The matters listed above have been included as matters that the court should have regard to as they are relevant to determining whether disclosure of the information would create a real risk of damage to the public interest. In practice, this may include disclosure which would pose an unacceptable risk to the intelligence capabilities, operations and sources of law enforcement and

intelligence agencies – including active investigations. This in turn may compromise Australia's national security. The matters listed above are relevant to the court's determination because the disclosure of the information may therefore risk jeopardising the trusted relationship between the Department and law enforcement and intelligence agencies, and may result in information that is relevant to character decisions not being made available to the decision-maker for consideration.

Additionally, while the listed matters include 'Australia's national security' explicitly (as per s52C(5)(g) of the Citizenship Act and s503C(5)(g) of the Migration Act), and will often involve national security issues directly or indirectly, they are broader than this provision alone. This is because the protection of sensitive and confidential information is intended to support the operational activities of law enforcement agencies as well as broader strategies to counter terrorism, transnational crime and related activities, including protection of informants and protection of technologies and methods.

The Bill will provide safeguards for the applicant by allowing the courts to decide how much weight to give to the confidential information that has been submitted in evidence (s52C(7) of the Citizenship Act and s503C(7) of the Migration Act). This allows the courts to weigh up a number of factors, including fairness to the applicant and the public interest when assessing what weight to attribute to the evidence. Practically, this may involve a situation where the court has determined not to disclose the protected information, which would include not disclosing the information to the applicant. Even so, the court is to weigh up a number of factors when assessing what weight to give to evidence, including unfair prejudice to an applicant by not having access to the confidential information as well as the public interest. Information available for the courts to consider in this regard would include any information that the applicant, their authorised representative or any third party has raised in support of their case, irrespective of whether the protected information has been disclosed to the applicant or their authorised representative.

- **why it is necessary and appropriate for the matters specified in proposed subsections 52C(5) and 503C(5) to be exhaustive;**

The measures in the Bill are necessary to strengthen the Government's ability to uphold public safety and the good order of the Australian community through character-related decisions made under both the Migration Act and the Citizenship Act.

These measures will enhance the ability of decision-makers to use confidential information to manage the risk of certain individuals of character concern, where there may otherwise be insufficient non-confidential information to underpin a decision. The changes help ensure that these individuals who pose a risk to public safety will be prevented from entering or remaining in Australia by providing a framework which protects the confidential information from harmful disclosure.

The potential disclosure of confidential information may pose an unacceptable risk to the intelligence capabilities, operations and sources of law enforcement and intelligence agencies – including active investigations. This risks jeopardising the trusted relationship between the Department and law enforcement and intelligence agencies, and may result in information that is relevant to character decisions not being made available to the decision-maker for consideration.

The framework proposed by the Bill provides a mechanism which allows the court to require disclosure of the relevant information to it and a further mechanism for the court to consider whether it can disclose the protected information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest.

It is appropriate that the list of matters the court can have regard to (if relevant) in subsections 52C(5) of the Citizenship Act and 503C(5) of the Migration Act is exhaustive, as it provides clarity and certainty for the court in exercising its functions. As noted above, the scope and content of the matters listed in those sections reflects and emphasises the sensitive nature of the information, and the need for the court to give careful consideration to those matters in order to decide whether there would be a real risk of damage to the public interest if the information was disclosed more widely, including to the applicant in judicial review proceedings.

The Bill provides that the court may give such weight in the substantive proceedings to the information as the court considers appropriate in the circumstances. Such circumstances may involve a situation where the court has determined not to disclose the protected information. This allows the courts to weigh up a number of factors, including unfair prejudice to an applicant by not having access to the confidential information and the public interest. This provides clear safeguards for the applicant's interests in any proceedings, and places these safeguards within the control of the court.

- **why it is not possible to allow the court to disclose the relevant information (or a summary of it) to the extent that is necessary to ensure procedural fairness in circumstances where partial disclosure could be achieved without creating a real risk of damage to the public interest;**

The Bill proposes a number of amendments to the Migration Act and the Citizenship Act to protect confidential information provided by gazetted law enforcement and intelligence agencies on the condition that it is treated as confidential for use in visa and citizenship decision-making, in order to enhance the Government's ability to manage risks to the community posed by certain individuals of character concern.

In practice, law enforcement and intelligence agencies provide confidential information to the Department of Home Affairs on the basis that it can be protected from disclosure. This is because, if such information were disclosed, there would be a real risk that there would be damage to the public interest and jeopardise the capabilities of law enforcement and intelligence agencies – and potentially compromise active investigations. Therefore, it is the agencies themselves who designate the information as confidential because of the intrinsically sensitive nature of its contents and scope.

Criminal intelligence and related information is vital to assessing the criminal background or associations of non-citizen visa and citizenship applicants and visa holders. The measures in this Bill will ensure that information – disclosed in confidence by law enforcement and intelligence agencies – is appropriately protected.

Given the sensitive nature of the information communicated in confidence by the gazetted agencies and the identity of the gazetted agency itself, partial disclosure of the information or of a summary of the information to the applicant could damage the public interest. Further, it is open to gazetted agencies to communicate information which they may indicate is not communicated in confidence. Where this occurs, the information would not be subject to the protected information framework and so may (subject to other relevant laws) be subject to full or partial disclosure, or disclosure of a summary, as appropriate.

The Minister considers that the current approach in the Bill is appropriate and that any consideration of whether to disclose part of the relevant information is duplicative and unnecessary: the same risks of damage to the public interest would arise from partial or full disclosure given the sensitive nature of the information in question.

Nonetheless, the Bill will provide for greater judicial oversight in visa and citizenship decisions that rely on confidential information. The amendments allow the courts to require the disclosure to it of confidential information provided by gazetted agencies that was relevant to the exercise of power by the Minister (or delegate) which is the subject of the proceedings.

The Bill will provide safeguards for the applicant by allowing the courts to decide how much weight to give to the confidential information. This allows the courts to weigh up a number of factors, including fairness to the applicant and the public interest, in using this information in review of visa and citizenship decisions. Practically, this may involve a situation where the court has determined not to disclose the protected information, which would include not disclosing the information to the applicant.

- **why procedural fairness, particularly as relates to the applicant, is not included as a matter that the court must have regard to when determining whether disclosing the information would create a real risk of damage to the public interest;**

The Bill, together with the existing framework as a whole, aims to strike an appropriate balance between protecting the public interest and providing fairness to the applicant.

- The Bill will allow confidential information provided by law enforcement and intelligence agencies to be considered by the courts while preventing its further disclosure where it would create a real risk of damage to the public interest.
- The Bill will provide safeguards for the applicant by allowing the courts to decide how much weight to give the confidential information in judicial review, and to further disclose this information when there is no real risk of damage to the public interest. Where the court has determined not to disclose the information, which would include not disclosing the information to the applicant, the court may take into account the unfair prejudice for the applicant when deciding what the weight to give to that information.

The matters listed in s52C(5) of the Citizenship Act and s503C(5) of the Migration Act are limited to those which could be broadly characterised as matters going to the public interest, as they reflect and emphasise the highly sensitive nature of the information provided by the gazetted agencies to the Department for use in character-related decision making. Noting this, the Bill also provides that the court may give such weight to protected information as is appropriate in the circumstances, which would include circumstances where the court has determined not to disclose the information to the applicant. This allows the court to consider the impact non-disclosure would have on the applicant when giving weight to evidence.

The Bill does not remove procedural fairness from character-related visa and citizenship decision making processes. Rather, procedural fairness is provided at the various stages of the process in a way that strikes an appropriate balance between protecting the public interest (by protecting confidential information provided by intelligence and law enforcement agencies) and providing fairness to the affected person.

Where a person seeks judicial review, the court will afford the affected person natural justice and the framework in s52C of the Citizenship Act and s503C of the Migration Act will be enlivened. This framework provides a mechanism which allows the court to require disclosure of the relevant confidential information to it and a further mechanism for the court to consider whether it can disclose the information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest. In this way, the court can exercise its judicial functions in order to conduct an effective judicial review.

- **what other matters are likely to be specified in the regulations in relation to proposed subsections 52C(5) and 503C(5);**

It is noted that paragraphs 52C(5)(h) of the Citizenship Act and 503C(5)(h) of the Migration Act provide a mechanism for other matters to be included in these subsections if specified in relevant regulations. These paragraphs were included in the Bill in order to provide flexibility going forward.

Given the rapidly evolving and complex security challenges, it is essential that further specifications are able to be made in the regulations to ensure the ongoing protection of confidential information shared between the Department, law enforcement and intelligence agencies in a changeable national security landscape. As such, if Parliament passes the Bill, the Department will monitor the operation of the protected information framework provided for in the Bill and, if deemed desirable or necessary to assist the court in determining whether to disclose the confidential information, to include further matters for the court to have regard to in subsections 52C(5) of the Citizenship Act and 503C(5) of the Migration Act. This can be effected through amendments to the *Australian Citizenship Regulation 2016* or *Migration Regulations 1994* , as appropriate. As amendments to these Regulations are disallowable, they will be accompanied by a Statement of Compatibility with Human Rights and subject to parliamentary scrutiny.

- **why is there no process by which a special advocate or equivalent safeguard is able to represent the applicant's interests if it is determined that relevant information be withheld from the applicant;**

The Bill will allow the courts to admit confidential information into evidence and to decide how much weight to give to that evidence.

This will sufficiently allow the courts to weigh up a number of factors, including prejudice to an applicant by not having access to the confidential information and the public interest.

The gazetted intelligence and law enforcement agencies are defined in the Bill at s503A(9) of the Migration Act (which is identical to the current s503A(9) of the Migration Act). The same definition applies within the context of the Citizenship Act. Gazetted agencies include Australian and foreign law enforcement or intelligence bodies which are listed in the Gazette. A war crimes tribunal established under international arrangements of law may also be a gazetted agency and is not required to be listed in the Gazette.

As such, the gazetted agencies are publicly identifiable. Effectively, this means that affected persons are on notice as to the identities of intelligence and law enforcement agencies that may communicate confidential information to the Department for use in character-related visa and citizenship decision making. This may help affected persons and their representatives understand where the confidential information may be sourced and to put forward relevant matters for the consideration of the court.

The framework in the Bill provides a mechanism which allows the court to require disclosure of the relevant confidential information to it and a further mechanism for the court to consider whether it can disclose the information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest. The Bill further provides that the courts may give such weight in the substantive proceedings to the information as the court considers appropriate in the circumstances. In this way, the court can exercise its judicial functions in order to conduct an effective judicial review.

- **what, if any, other safeguards exist to ensure that the proposed limit on the right to a fair trial and the prohibition against expulsion without due process are proportionate.**

The limitations on providing all of the information to the affected person are in place to strengthen the Government's ability to uphold public safety and the good order of the Australian community through character-related visa and citizenship decisions and to protect highly sensitive information communicated in confidence by gazetted agencies when used in making those decisions. The affected person will continue to have the ability to submit reasons against their expulsion in a merits and/or judicial review process. Further, in the judicial review of those decisions, the court will be able to consider the information, whether disclosure would create a real risk of damage to the public interest, and how much weight to accord to information that it knows has not been made available to the affected person.

Specifically, the framework will provide that during judicial review, the courts may order the Minister to disclose confidential information to it that was relevant to the visa or citizenship decision (that is, the Minister will not have a discretion not to comply in this circumstance). The Minister can provide submissions to the courts about the use of the information and the impact that further disclosure would have on the public interest.

As noted elsewhere, the Bill provides that the courts may give such weight in the substantive proceedings to the information as the court considers appropriate in the circumstances. Such circumstances may involve a situation where the court has determined not to disclose the protected information. This allows the courts to weigh up a number of factors, including unfair prejudice to an applicant by not having access to the confidential information and the public interest. This provides clear safeguards for the applicant's interests in any proceedings and places these safeguards within the control of the court.

Further, existing merits review rights will not be affected by the Bill. The Minister has long had power to disclose or protect information from disclosure during merits review. The Bill will provide the Minister with discretionary powers to disclose the confidential information (having consulted the relevant gazetted agency) to specified persons, bodies, tribunals or courts.

Where the Minister does authorise disclosure of protected information to a Tribunal in accordance with s52B(1) of the Citizenship Act and s503B(1) of the Migration Act, then the Tribunal will have obligations to afford natural justice during any relevant merits review subject to the obligations imposed upon it by s52B of the Citizenship Act and s503B of the Migration Act.

The balance reflected in the Bill will enable law enforcement agencies to continue to provide confidential information to the Department to make fully informed visa and citizenship decisions on character grounds, while providing fairness to applicants seeking merits or judicial review of a departmental decision. This is essential to the Government's core business of regulating, in the national interest, who should enter and remain in Australia, and who should be granted Australian citizenship and the privileges which attach to it.

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

Ref No: MS21-000229

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

Dear Sarah, ~~Ms~~ Henderson

Thank you for your letter dated 4 February 2021 requesting my response in relation to the human rights compatibility of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020.

I note the Committee has sought further information regarding the compatibility of the proposed measures with Australia's international human rights obligations.

My response for the Committee's consideration is attached. I appreciate the extension until 23 February in which to provide the response.

Yours sincerely

PETER DUTTON 19/02/21

Response to the Parliamentary Joint Committee on Human Rights

Scrutiny Report 1 of 2021

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Right to privacy

1.77. In order to assess the compatibility of this measure with the right to privacy, in particular the adequacy of existing safeguards, further information is required as to:

a. why the power to issue a data disruption warrant and network activity warrant is conferred on a member of the AAT, of any level and with a minimum 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

In the Bill, the power to issue data disruption warrants and network activity warrants is conferred on an eligible Judge or a nominated Administrative Appeals Tribunal (AAT) member. These issuing authorities may grant the warrant if (amongst other things) they are satisfied that there are reasonable grounds for the suspicion founding the application for the warrant. This independent scrutiny of warrant applications is an important mechanism in ensuring that only warrants that are reasonable and proportionate are issued, and that the power is consistent with Australia's international human rights law obligations.

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 existing legislation including the *Surveillance Devices Act 2004* (SD Act) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

AAT members have the experience and skills necessary to issue data disruption warrants and network activity warrants

Both AAT members and judges play critical roles as independent decision-makers in authorising investigatory powers in the current regimes in the SD Act, as well as in the TIA Act. Nominated AAT members issue surveillance device warrants and computer access warrants under the SD Act, and have played a key role in issuing interception warrants under the TIA Act since 1998. The skills and experience of AAT members make them suitable to assess applications for data disruption warrants and network activity warrants, and whilst doing so, to make independent decisions on the compliance of those applications with the legal requirements in the Bill.

To be nominated as an AAT member for the purposes of issuing warrants under the SD Act, a person must have been enrolled as a legal practitioner for at least five years. In accordance with the existing framework, the Bill recognises that the complex decision-making involved in authorising the new powers in the Bill requires the independence offered by the AAT members and judges who already issue other warrants under those Acts and have the skills and experience to do so.

AAT members are independent decision-makers

The power to issue warrants is conferred on issuing authorities in their personal capacity (*persona designata*) as a means of ensuring accountability in the course of a sensitive investigation or law enforcement procedure. *Persona designata* functions are not an exercise of the formal judicial or administrative powers of a court or tribunal. Rather these issuing authorities are acting as independent decision-makers.

The AAT is not independent of government in the same way that the judiciary is the subject of a separation of powers (though some members of the AAT are also judges). Rather, the AAT's independence arises from its role in reviewing the merits of administrative decisions made under Commonwealth laws. The independence of the AAT is also demonstrated in the process for the termination of a member's appointment. AAT members who are not judges can only have their

appointment terminated by the Governor-General, and this termination can only be made on specific grounds, such as proven misbehaviour or the inability to perform duties.

The independence of AAT members exercising *persona designata* functions is strongly safeguarded. AAT members are afforded the same protection and immunity as a Justice of the High Court of Australia, and they must provide written consent prior to being authorised to perform *persona designata* functions. Consent also serves to protect an AAT members' independence and autonomy to decide whether or not to exercise *persona designata* powers.

Review of administrative decisions

In the unlikely event of unlawful decision-making, Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 39B(1) of the *Judiciary Act 1903*, or under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). There is an error in the human rights compatibility statement in the explanatory memorandum supporting the Bill, which states that the Bill excludes judicial review under the ADJR Act. This is incorrect, and the human rights compatibility statement will be amended accordingly. These judicial review mechanisms ensure that an affected person has an avenue to challenge the decisions to issue warrants made by any issuing authorities, including a nominated AAT member.

As such, the Government maintains that the persons eligible to issue data disruption warrants and network activity warrants should not be limited to only judicial officers, but should include nominated AAT members, in line with the existing legislation.

b. why the bill does not require, in relation to all warrants, that the issuing authority must consider the extent to which the privacy of any person is likely to be affected, noting that as drafted, this consideration only applies to account takeover warrants

c. why the bill does not require, in relation to all warrants, that the issuing authority must consider whether the warrant is proportionate having regard to the nature and gravity of the offence and the likely value of the information or evidence sought to be obtained, as well as the extent of possible interference with the privacy of third parties, noting that as drafted, these considerations only apply to network activity warrants

In deciding whether to issue each of the warrants in the Bill, there are certain matters which the issuing authority must take into account. These considerations have been specifically designed with regard to the objective and contemplated operation of each of the warrants.

Proportionality test for data disruption warrants

In order to issue a data disruption warrant, the Judge or AAT member must be satisfied that, amongst other things, the disruption of data authorised by the warrant is justifiable and proportionate with regard to the offences targeted. This is to ensure that in considering whether to issue the warrant, the issuing authority weighs up the benefits of targeting the particular offences that the proposed data disruption seeks to frustrate, with the likely effect that data disruption could have beyond frustrating those offences. Satisfaction that the execution of the warrant is justifiable assists in satisfying the requirement under international human rights law that the limitation on the right to privacy is reasonable and not arbitrary.

A specific requirement that the issuing authority consider the privacy of third parties is not appropriate in the context of data disruption warrants, even though it is appropriate in the context of other electronic surveillance warrants the purpose of which is the gathering of evidence. Data disruption warrants are for the purpose of frustrating criminal activity, including preventing further harm to victims, stopping criminal offences occurring, and re-directing activity so that agencies can take appropriate action. It may not always be possible, at the time of applying for the warrant, for an agency to estimate the full extent to which activity required to undertake data disruption is likely to have an impact on third parties. In light of this, rather than providing for an express privacy consideration the Bill contains a mandatory condition that the issue of a data disruption warrant be justified and proportionate having regard to the offences targeted. To further ensure that these warrants are proportionate to the activity they authorise,

the issuing authority must consider the existence of any alternative means of frustrating the criminal activity.

There is no requirement that in considering whether to issue a data disruption warrant, the issuing authority take into account the likely evidentiary value (or intelligence value) of the information sought under the warrant. This is because data disruption warrants are not for the purposes of collecting evidence (or intelligence). Data disruption warrants are for the purposes of frustrating criminal offences.

Proportionality test for network activity warrants

In order to issue a network activity warrant, the Judge or AAT member must consider whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer. The issuing authority must also consider the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant. The purpose of network activity warrants is to allow the AFP and ACIC to target the activities of criminal networks to discover the scope of criminal offending and the identities of the people involved. Due to the complexity of the threats posed by cyber-enabled crime, it is unlikely that agencies will know in advance the identity or location of the offenders involved in the commission of offences to which the network activity warrant is related.

Network activity warrants are an intelligence collection tool and the information collected cannot be used in evidence in criminal proceedings. As such, the considerations for issue of a network activity warrant differ from those in relation to warrants that are issued for the purposes of gathering evidence (for example, computer access warrants in the SD Act). Intelligence collection by its nature is less targeted than evidence-gathering. Using a network activity warrant, the AFP or ACIC may need to collect intelligence on a large number of unknown devices, the users and owners of which are not able to be identified or located, before seeking more targeted warrants that authorise gathering evidence (such as computer access warrants under the SD Act). It will be difficult, if not impossible, for an issuing authority to assess the privacy implications for multiple unknown persons to a sufficient degree to meet the threshold of a specific requirement to consider the privacy of third parties. Instead, the issuing authority must consider the extent to which the execution of a network activity warrant is likely to result in access to data of persons who are lawfully using a computer. The proportionality test requires that the issuing authority weigh up the anticipated value of the intelligence sought with the activities authorised by the warrant. This ensures that the issuing authority must balance the utility of the network activity warrant in obtaining information about the criminal network against the scale, scope and intrusiveness of the activities authorised by that warrant. To further ensure that these warrants are proportionate to the activity they authorise, the issuing authority must consider the existing of any alternative or less intrusive means of obtaining the information sought.

Privacy consideration for account takeover warrants

For account takeover warrants, the magistrate must consider the extent to which the privacy of any person is likely to be affected. An explicit privacy consideration is appropriate for the issue of account takeover warrants as it is a targeted evidence gathering power. This is consistent with the approach for existing electronic surveillance powers, such as those in the SD Act.

When deciding whether to issue the warrant, the magistrate must also have regard to the nature and gravity of the alleged offence that founded the application for the warrant. This may involve consideration of the seriousness of the offence and the scale at which the offence has been, or will be, committed. Consideration of this matter ensures that the magistrate will be able to assess the reasonableness and proportionality of executing the warrant in the circumstances. If the offence for which the warrant is sought is not sufficiently serious to justify the conduct of an account takeover warrant and its impact on privacy, the magistrate can decide not to issue the warrant.

d. how the qualification that the statutory conditions do not limit the conditions to which a data disruption warrant or account takeover warrant may be subject would operate in practice. In particular, would this qualification allow an issuing authority to authorise an action that can only be executed in a manner that results in loss or damage to data or causes the permanent loss of money, digital currency or property

The Bill provides for statutory conditions to which data disruption warrants and account takeover warrants must be subject. These conditions place limitations on the execution of the warrant. If the warrant is executed in a way that breaches the statutory condition then that conduct would be unlawful, as it is not supported by the warrant. As identified by the Committee, the Bill provides that the statutory conditions do not limit the conditions to which a data disruption warrant or an account takeover warrant may be subject. This refers to the ability of the issuing authority to specify any conditions subject to which things may be done under the warrant (subparagraph 27KD(1)(b)(ix) in the SD Act and subparagraph 3ZZUQ(1)(b)(ix) of the Crimes Act). The statutory conditions do not restrict the issuing authority's ability to prescribe additional conditions under those provisions, to which the execution of the warrant would then also be subject.

As noted by the Committee, the statutory conditions provide that if loss or damage to data occurs during the execution of a warrant, the damage must be justified and proportionate to the offence being targeted by the warrant. Whether loss or damage that may possibly occur during execution of the warrant is justified and proportionate will need to be considered by the issuing authority on a case-by-case basis. Warrants must also not be executed in a manner that causes a person to suffer a permanent loss of money, digital currency or property (other than data). This is intended for an abundance of clarity about the scope of the warrants. Interference with a person's money, digital currency or property that is not data is not the intended purpose of either of these warrants. The issuing authority's ability to prescribe additional conditions does not allow authorisation of an action that can only be executed in a manner that results in loss or damage to data or causes the permanent loss of money, digital currency or property.

e. whether all of the exceptions to the restrictions on the use, recording or disclosure of protected information obtained under the warrants are appropriate and whether any exceptions are drafted in broader terms than is strictly necessary

All information collected under the warrants in this Bill is strictly protected. Information is broadly prohibited from being used or disclosed. Where there are exceptions to that prohibition, those exceptions are necessary to enable the warrants to be effective, strong oversight and accountability mechanisms, proper and appropriate judicial processes to be carried out, information sharing necessary for agencies to carry out their functions, or in emergency circumstances. The ability to use and disclose information has been designed to be limited to only that which is necessary.

Prohibition and offences

The Bill classifies data disruption warrant information as 'protected information' under the existing provisions in the SD Act, which currently govern information collected under other warrants in that Act, for example, computer access warrants.

Information gathered under an account takeover warrant is also classified as 'protected information'. This is a new concept in the Crimes Act introduced by the Bill, borrowing from the SD Act, so that account takeover warrant information is governed by the same prohibitions and exceptions as most information under the SD Act, including data disruption warrant information.

There is also a prohibition on using and disclosing 'protected network activity warrant information', a new category of protected information introduced by the Bill into the SD Act. Protected network activity warrant information is information obtained under, or relating to, a network activity warrant including information obtained from the use of a surveillance device under a network activity warrant but not including information obtained through interception. This also includes any information that is likely to enable the identification of the criminal network of individuals, individuals in that network, computers used by that network, or premises at which computers used by that network are located. Information

that was obtained in contravention of a requirement for a network activity warrant is also captured by this definition.

A person commits an offence if he or she uses, records, communicates or publishes protected information or protected network activity warrant information except in very limited circumstances. The Bill also provides for an aggravated offence if this disclosure endangers the health or safety or any person or prejudices the effective conduct of an investigation.

Exceptions – data disruption warrants and account takeover warrants

The exceptions to the prohibition on using, recording, communicating or publishing information collected under a data disruption warrant and under an account takeover warrant are the same as exceptions in the SD Act that relate to existing warrants, such as computer access warrants.

It is permitted to use, record, communicate, publish, and admit in evidence, protected information where necessary for the investigation of a relevant offence, a relevant proceeding, or the making of a decision as to whether or not to bring a prosecution for a relevant offence (amongst other limited purposes). It is also permitted to use, record, communicate or publish protected information where that information has already been disclosed in proceedings in open court lawfully, and where the communication of the information is necessary to help prevent or reduce the risk of serious harm.

Information collected under each of these warrants may also be shared with an intelligence agency if the information relates to a matter that is relevant to the agency's functions, and with a foreign country, the International Criminal Court, or a War Crimes Tribunal under international assistance authorisations, and also where authorised by the *Mutual Assistance in Criminal Matters Act 1987* or the *International Criminal Court Act 2002*. It is essential that this information sharing is permitted, in order to facilitate investigations that involve other Australian agencies (for example conducting joint operations) and foreign jurisdictions. Further information is outlined below, as requested by the Committee, on the right to privacy, life and prohibition against torture or cruel, inhuman or degrading treatment or punishment, in the context of the Bill's framework for information sharing with foreign countries.

Information may also be shared with the Ombudsman and the IGIS, and between those agencies to allow them to fulfil their oversight responsibilities in relation to the powers in the Bill.

Exceptions – network activity warrants

The exceptions to the general prohibition on using and disclosing protected network activity warrant information are configured differently to those relating to data disruption warrants and account takeover warrants. This is because, as network activity warrants are for intelligence purposes, they cannot be used to gather evidence in investigations, and the information collected generally cannot be adduced in evidence in a criminal proceeding.

Protected network activity warrant information may be used or disclosed if necessary for collecting, correlating, analysing or disseminating, or the making of reports in relation to, criminal intelligence in the performance of the legislative functions of the AFP or the ACIC. The information can also be the subject of derivative use allowing it to be cited in an affidavit on application for another warrant (which will themselves contain protections on information gathered). This will assist in ensuring that network activity warrants can be useful in furthering investigations into criminal conduct made under subsequent warrants.

Protected network activity warrant information cannot be used in evidence in criminal proceedings, other than for a contravention of the secrecy provisions that apply to this intelligence. This is important for ensuring that where a person has unlawfully used or disclosed this information, he or she may be effectively investigated and prosecuted for the offence. The information may also be disclosed for the purposes of the admission of evidence in a proceeding that is not a criminal proceeding. This is intended to allow protected network activity warrant information to be used in other proceedings, such as those that question the validity of the warrant. Therefore, if a case is brought to challenge the decision to issue a warrant, there will be evidence which can be validly drawn upon. These exceptions are intended to

protect the rights of persons who are the subject of, or whose information has been collected under, a network activity warrant.

The ability to share information obtained under a network activity warrant with ASIO or an intelligence agency is intended to facilitate joint operations between the AFP and the ACIC and other members of the National Intelligence Community. These agencies currently conduct complex and interrelated intelligence operations, and may need to share information to support activities within their respective functions, in particular those in relation to safeguarding national security. For example, information collected under a network activity warrant about a terrorist organisation may be shared with ASIO if related to ASIO's functions. Information held by ASIO and intelligence agencies, including information obtained under a network activity warrant that is then communicated to those agencies, is protected by strict use and disclosure provisions in the *Australian Security Intelligence Organisation Act 1979* and *Intelligence Services Act 2001*.

To ensure compliance with reporting and record-keeping requirements, the Bill provides that protected network activity warrant information may be used or disclosed for the purpose of keeping records and making reports by the AFP and the ACIC in accordance with the obligations imposed by the Bill. Information may also be shared with the Ombudsman and the IGIS, and between those agencies to allow them to fulfil their oversight responsibilities in relation to the powers in the Bill. These exceptions are important to facilitate effective oversight of the AFP and the ACIC and protect the rights of persons who are the subject of, or whose information has been collected under, a network activity warrant. Information held by the Ombudsman and IGIS, including information obtained under a network activity warrant that is then communicated to those bodies, is protected by strict use and disclosure provisions in the *Ombudsman Act 1976* and *Inspector-General of Intelligence and Security Act 1986*.

f. why the bill does not include provision for public interest monitors or a similar safeguard to protect the rights of the affected person in warrant application and review proceedings

Consistent with covert powers available to the AFP and the ACIC under existing legislation, the Bill does not make provision for public interest monitors to assess applications for warrants before they can be issued. In particular, this is in accordance with the approach for surveillance device warrants and computer access warrants in the SD Act. At present, public interest monitors recognised under the TIA Act only exist within Victoria and Queensland, as a corollary of Victorian and Queensland legislation that established those offices within those jurisdictions, for functions that include but are not limited to considering Victorian and Queensland agency applications for interception warrants. These authorities perform an oversight role of their jurisdiction's law enforcement agencies when applying for interception warrants. The Commonwealth, and other States and Territories, have not legislated for this office within their jurisdictions.

To protect the rights of an affected person, the warrants in the Bill are supported by a range of safeguards, stringent thresholds and oversight arrangements which ensure that they may only be sought where reasonable, proportionate and necessary.

Each of the warrants can only be applied for by the AFP or the ACIC on the basis of a link to serious offending. Specifically, the warrants must be sought in respect of *relevant offences*, that is, generally offences punishable by a maximum term of imprisonment of three years or more. This threshold limits the availability of data disruption warrants, network activity warrants and account takeover warrants to serious crimes, such as terrorism, child exploitation and drugs and firearms trafficking.

All of the warrants in the Bill must be sought by way of application to a judicial officer or AAT member, who may grant the warrant sought if they are satisfied that there are reasonable grounds for the suspicion founding the application for each warrant. Oversight of decisions to apply for warrants by judicial officers and AAT members provides for independent scrutiny of the warrant application and satisfaction of reasonableness and proportionality.

As described above, a key matter that the issuing authority is required to take into account in deciding whether to issue each of the warrants is consideration of proportionality. The issuing of a data disruption warrant or network activity warrant must meet a proportionality test. This is to ensure that the use of

these warrants is proportionate to the alleged or suspected offending in all circumstances. An explicit privacy consideration is included for the issue of account takeover warrants as it is a targeted evidence gathering power.

Central amongst other considerations that issuing authorities must take into account is consideration of the existence of any alternative means of achieving the objective of the warrant. These safeguards are particularly important for ensuring that avenues of investigation, information collection or disruption that are less intrusive on privacy are considered. This ensures that, where there are narrower activities that involve a more targeted approach, this will be taken into account by the issuing authority.

Moreover, decisions made in regard to the issue of warrants in the Bill can be challenged through judicial review. Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and under the ADJR Act. This will ensure that an affected person has an avenue to challenge the decisions to issue warrants made by issuing authorities. The availability of judicial review is discussed in further detail below.

As with other evidence-gathering powers in the SD Act and Crimes Act, the Commonwealth Ombudsman will have oversight of the use of data disruption warrants and account takeover warrants by the AFP and the ACIC. The Bill provides for oversight of network activity warrants by the Inspector-General of Intelligence and Security. The IGIS will be empowered to review the activities of the AFP and the ACIC in relation to network activity warrants for legality, propriety and consistency with human rights. This is consistent with the IGIS's oversight of other agencies' intelligence collection powers.

g. why the chief officer is not required to review the continued need for the retention of records or reports comprising protected information on a more regular basis than every five years

Records comprising protected information in the Bill must be destroyed as soon as practicable if the material is no longer required, and at most within five years of the material no longer being required (unless a relevant officer certifies certain matters that go to the need to keep the material for ongoing activity). As noted by the Committee, the chief officer of the AFP or the ACIC must ensure that information obtained under each of these warrants is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. This is consistent with existing record-keeping and destruction obligations in relation to surveillance device warrants and computer access warrants in the SD Act.

As with information collected under existing warrants in the SD Act, the ability to retain information for five years reflects the fact that some investigations and operations are complex and run over a long period of time. Requiring the security and destruction of records ensures that the private data of individuals accessed under a warrant is only handled by those with a legitimate need for access, and is not kept in perpetuity where there is not a legitimate reason for doing so. The Ombudsman and IGIS are empowered to assess compliance with record-keeping and destruction requirements as part of their oversight of powers in the Bill.

Right to an effective remedy

1.82. In order to assess whether any person whose right to privacy might be violated by the proposed warrants would have access to an effective remedy, further information is required as to:

a. whether a person who was the subject of a warrant will be made aware of that after the investigation has been completed

In accordance with existing practice for covert powers under Commonwealth legislation, persons of interest or those who are subject to the new covert warrants in the Bill do not have to be notified of the use of powers against them unless there is a specific requirement under law to do so. This is consistent practice for covert warrants under the SD Act and other Commonwealth legislation that confers covert powers upon law enforcement and security agencies, such as the TIA Act.

If a person were to become aware of the use of a covert warrant while an investigation or operation is ongoing, this could place law enforcement outcomes at risk by tipping off those engaging in criminal conduct about the investigation or operation and, potentially, the capabilities and methodologies being employed. Notifying a person after the conclusion of an investigation or operation can also have significant ramifications for future law enforcement methodologies and the legitimate need to keep technical capabilities that relate to electronic surveillance confidential.

Public disclosure of the details of a covert warrant 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 being monitored under a network activity warrant may mean that many months or years of law enforcement efforts to penetrate criminal networks (such as online child sexual abuse groups) can be lost. This ultimately reduces the effectiveness of the AFP and the ACIC to keep the Australian community safe from serious online crime.

Even where the subject of a warrant has been cleared of any criminal activity, this does not necessarily reduce the risk that the disclosure may impact future law enforcement methodologies and protection of technical capabilities. For example, the person who holds the account subject to an account takeover warrant could inadvertently jeopardise future law enforcement investigations by publicly announcing they were subject to the warrant in relation to an account on a particular electronic service.

While the Government acknowledges that the use of a covert warrant will impact a person's privacy, this limitation is reasonable, necessary and proportionate in order to safeguard the Australian community from serious crime. These measures are balanced with strict safeguards, including restrictions on the use and disclosure of information obtained under a warrant, and robust oversight and reporting requirements. In particular, the Commonwealth Ombudsman and the IGIS will inspect and review agencies' use of the warrants in the Bill.

b. 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 a warrant in the Bill, measures are in place to protect an individuals' right to privacy and right to an effective remedy. The Bill balances the impact on privacy and the covert nature of powers by ensuring independent authorisation of warrants, as well as effective oversight, record-keeping and reporting. In particular, there is aggregated public annual reporting on the AFP and ACIC's use of powers in the Bill.

Importantly, a person who is the subject of a warrant can challenge decisions made in regard to data disruption warrants, network activity warrants and account takeover warrants through judicial review. As these are covert powers, in practice the challenge to these decisions will likely only be if and when the particular investigation has become overt. For example, a person who is the subject of a warrant may become aware of this during the preparation for or conduct of criminal proceedings.

To make information available in order to bring about such a challenge, the Bill ensures that, although network activity warrants are not for evidence collection and therefore there are strict prohibitions on adducing that information in evidence in proceedings, information obtained under a network activity warrant may be admitted into evidence in proceedings that are not criminal proceedings. This is an important exception to the general secrecy provisions that apply to covert intelligence gathering activities. The Bill also applies the same exception to information gathered under an account takeover warrant.

Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 39B(1) of the *Judiciary Act 1903*. This will ensure that an affected person has an avenue to challenge the decisions to issue warrants made by issuing authorities. The availability of judicial review is discussed in further detail below.

As outlined above, decisions made under the SD Act and the Crimes Act are <u>not</u> exempt from judicial review under the ADJR Act. The Bill does <u>not</u> seek to depart from this precedent for the three new

warrant it introduces. The human rights compatibility statement in the explanatory memorandum supporting the Bill will be amended to reflect this.

While judicial review is available, agency decisions to exercise a power and issuing authority decisions to issue warrants are not subject to merits review. This is consistent with longstanding principles and practice relating to national security legislation and powers.[1] However, a defendant may seek to challenge evidence obtained under a warrant, should this evidence be used in the course of an eventual prosecution.

The use of powers in the Bill will be independently overseen by the Commonwealth Ombudsman (for data disruption warrants and account takeover warrants) and the IGIS (for network activity warrants). While this is not a merits review process, these oversight bodies play an important role in auditing and inspecting the records of agencies which increases transparency and accountability, and monitors and encourages compliance with the legislative requirements in the Bill.

Assistance orders – right to privacy

1.94. In order to assess the compatibility of this measure with the right to privacy, in particular the adequacy of the safeguards that apply, further information is required as to:

a. **why the issuing authority is not required to be satisfied that an assistance order is justifiable and proportionate, having regard to the offences to which it would relate, with respect to all warrants, noting that this criterion only applies to an assistance order with respect to data disruption warrants**
b. **whether the measure is accompanied by any other safeguards that would ensure that any interference with the right to privacy is not arbitrary and only as extensive as is strictly necessary.**

As the committee notes, an eligible Judge or nominated AAT member must be satisfied that disruption of data held in a computer is justifiable and proportionate, having regard to the offences targeted, before granting an assistance order in support of a data disruption warrant. This is because the criterion upon which the granting an assistance order is assessed reflects the criterion of which the issuing authority must be satisfied when authorising the supporting warrant.

In order to issue a data disruption warrant, an eligible Judge or nominated AAT member must (amongst other things) be satisfied that there are reasonable grounds for the suspicion of the law enforcement officer who made the warrant application that the disruption of data is likely to substantially assist in frustrating the commission of relevant offences. The eligible Judge or nominated AAT member must also be satisfied that the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences targeted (subsection 27KC(1) of the SD Act).

These are similar conditions for which an eligible Judge or nominated AAT member must be satisfied of when granting an assistance order in support of a data disruption warrant (subsection 64B(2) of the SD Act). Satisfaction of the similar matters at the time of issuing the warrant and the granting of the assistance order ensures that any activity required by an assistance order does not extend beyond the scope of the underpinning warrant.

The same principles apply in relation to the granting of assistance orders supporting network activity warrants and account takeover warrants. Similar matters that must be satisfied at the time of issuing these warrants must again be satisfied at the granting of an assistance order.

In recognition of the impact on privacy of third parties, the issuing authority is required to have regard to certain specified matters when deciding whether to issue the warrant. For network activity warrants, this includes consideration of whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer. For account takeover warrants, this includes taking

[1] Decisions of a law enforcement and national security nature were identified by the Administrative Review Council in its publication 'What decisions should be subject to merits review as being unsuitable for merits review'.
https://www.arc.ag.gov.au/Publications/Reports/Pages/Downloads/Whatdecisionsshouldbesubjecttomeritreview 1999.aspx

into account the extent to which the privacy of any person is likely to be affected. Consideration of these matters will inform the issuing authority's decisions to issue warrants, including his or her satisfaction of the matter particular to that warrant and, in turn, inform decisions about whether to grant an assistance order. Ensuring that the issuing authority is required to be satisfied of justifiability and proportionality before a warrant can be issued or assistance order granted is intended to safeguard against any undue impact on privacy.

Information sharing with foreign governments – right to privacy, life and prohibition against torture or cruel, inhuman or degrading treatment or punishment

1.106. In order to fully assess the compatibility of the measure with the rights to privacy and life as well as the prohibition against torture or cruel, inhuman or other degrading treatment or punishment, further information is required as to:

a. **what is the objective being pursued by the measure and how is the measure rationally connected to that objective**
b. **what safeguards are in place to ensure that protected information obtained under the warrants is not shared with a foreign country in circumstances that could expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment. In particular, why is there no legislative requirement that where there are substantial grounds for believing there is a real risk that disclosure of information to a foreign government may expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment, protected information must not be shared with that government**

As noted by the Committee, the Bill provides that information obtained under these warrants may be shared with foreign governments in certain limited circumstances. The AFP's primary aim is to enforce Commonwealth criminal law and contribute to combatting complex, transnational and organised crime which impacts on the Australian community and Australia's national interests. The AFP collaborates with national and international partners to enhance the safety of the Australian community and provide a more secure regional and global environment. The ACIC works to identify new and emerging serious and organised crime threats and criminal trends, to create a national strategic intelligence picture across the spectrum of crime, fill intelligence and knowledge gaps and share information and intelligence holdings to inform national and international responses to crime. This necessarily requires cooperation between the AFP and the ACIC and foreign police and law enforcement agencies. The ACIC has a specific power in the *Australian Crime Commission Act 2002* (Cth) (ACC Act), its underpinning legislation, in support of this collaboration. [2]

The criminal activity targeted by the Bill – serious crime occurring on the dark web or facilitated by anonymising technology – is an increasing global problem. Cooperation with foreign law enforcement partners can be crucial to identifying and targeting criminal activity which harms the Australian community, as well as building a high-risk, hostile environment for cyber criminals both onshore and offshore. That is why the Bill ensures that the AFP and the ACIC will be able to share information obtained under the warrants with foreign governments in accordance with their existing functions.

Importantly, in cooperating with foreign law enforcement agencies, the AFP and the ACIC operate in accordance with Australia's longstanding bipartisan opposition to the death penalty and the existing death penalty safeguards across the full spectrum of Australia's international crime cooperation frameworks.

For example, there are a number of safeguards that apply when cooperating with foreign countries through the mutual assistance framework. Provision of any evidentiary material, including protected information, to a foreign country is subject to the requirements of the *Mutual Assistance in Criminal Matters Act 1987*. A request for assistance must be refused where (i) a person has been arrested, detained, charged or convicted in relation to an offence where the death penalty may be imposed in the

[2] See s17(2) *Australian Crime Commission Act 2002* (Cth) (ACC Act)

foreign country, and (ii) where there are substantial grounds for believing that, if the request were granted, a person would be in danger of being subjected to torture.

In addition to the protections which apply under the Bill in relation to the disclosure of information to foreign agencies, section 59AA of the ACC Act contains additional safeguards. Under section 59AA, the authorising officer must be satisfied that the disclosure is appropriate and the information is relevant to a permissible purpose as defined in section 4 of the ACC Act. In considering whether a disclosure will be appropriate, amongst other factors, the authorising officer must take into account the ACIC Death Penalty and Foreign Disclosure Policy (which aligns to the AFP's *Practical Guide on international police-to-police assistance in potential death penalty situations*) where:

- A member of the staff of the ACIC proposes that information be disseminated to a foreign agency or international body or otherwise disclosed to a foreign official;
- The information relates to an offence that may have been committed and that could be prosecuted in the home country of the agency or official, or in a country to which the international body might be expected to disclose the information (the foreign country);
- Under the law of the foreign country, the offence is a death penalty offence; unless:
    - No person has been arrested, detained, charged or convicted for the offence in the foreign country; and
    - Providing the information is not reasonably likely to result in a person being arrested, detained, charged or convicted for the offence in the foreign country.

On a police-to-police basis, the AFP has strict national guidelines which govern the provision of information in situations which could expose a person to the death penalty. The AFP's *Practical Guide on international police-to-police assistance in potential death penalty situations* requires Ministerial approval of assistance in any case in which a person has been arrested, detained, charged with, or convicted of, an offence that carries the death penalty. Where a person is yet to be arrested, detained, charged or convicted of a death penalty offence, the Guide requires senior AFP management to consider a set of prescribed factors before providing police assistance to foreign countries. Examples of these factors include the age and personal circumstances of the person and the seriousness of the suspected criminal activity. In particular, these guidelines were updated in 2016 to response to recommendations made by the Joint Standing Committee on Foreign Affairs, Defence and Trade in its report '*A world without the death penalty: Australia's advocacy for the abolition of the death penalty.*'