Chapter 2

Concluded matters

2.1 This chapter considers responses to matters raised previously by the committee. The committee has concluded its examination of these matters on the basis of the responses received.

2.2 Correspondence relating to these matters is available on the committee's website.[1]

Bills

Biosecurity Amendment (Strengthening Biosecurity) 2022[2]

Purpose	This bill seeks to amend the *Biosecurity Act 2015* (the Biosecurity Act) to enable the minister to determine certain biosecurity measures and requirements for individuals entering Australian territory; establish and increase civil and criminal penalties for breaches to the Biosecurity Act; expand pre-arrival reporting requirements for aircraft and vessels; and provide for the use and disclosure of certain information, including protected information
Portfolio	Agriculture, Fisheries and Forestry
Introduced	House of Representatives, 28 September 2022 *Received Royal Assent 5 December 2022*
Rights	Health; privacy; freedom of movement; liberty; equality and non-discrimination; culture

2.3 The committee requested a response from the minister in relation to the bill in *Report 6 of 2022*.[3]

1 See https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports.

2 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Biosecurity Amendment (Strengthening Biosecurity) Bill 2022, *Report 1 of 2023*; [2023] AUPJCHR 10.

3 Parliamentary Joint Committee on Human Rights, *Report 6 of 2022* (24 November 2022), pp. 16-33.

Entry requirements

2.4 The bill, which is now an Act, confers new powers on the Agriculture Minister to determine, by exempt legislative instrument,[4] one or more entry requirements for individuals or classes of individuals who are entering Australian territory at a landing place or port.[5] The kinds of requirements that may be specified include requiring an individual to provide certain information by way of a declaration, be screened by equipment or in any other way, or move to a certain place for the purposes of a biosecurity risk assessment, whereby a biosecurity officer would assess the level of biosecurity risk associated with the individual and/or their goods and baggage.[6]

2.5 Before making an entry requirement, the minister must be satisfied that a disease or pest poses an unacceptable level of biosecurity risk; and the requirement is appropriate and adapted to prevent, or reduce the risk of, the disease or pest entering, establishing itself or spreading in Australian territory or part of Australian territory.[7] The minister is also required to consult with certain persons, including the Directors of Biosecurity and Human Biosecurity, before making a determination, although failure to do so would not affect the validity of the determination.[8] Failure to comply with an entry requirement would attract a civil penalty of 120 penalty units (currently $26,640).[9] A person may also commit an offence or contravene a civil penalty provision if they provide false or misleading information or documents.[10]

---

4 Schedule 1, item 5, proposed subsection 196A(4) provides that a determination made under this section is a legislative instrument but the disallowance provision (section 42 of the *Legislation Act 2003*) does not apply to the instrument. The Senate Standing Scrutiny of Bills and Scrutiny of Delegated Legislation Committees have previously raised concerns regarding the use of exempt legislative instruments under the *Biosecurity Act 2015*. See Senate Standing Committee for the Scrutiny of Bills, Review of exemption from disallowance provisions in the Biosecurity Act 2015, *Scrutiny Digest 7 of 2021* (12 May 2021), chapter 4, pp. 33–44; *Scrutiny Digest 1 of 2022* (4 February 2022), chapter 4, pp. 76–86; Senate Standing Committee for the Scrutiny of Delegated Legislation, Exemption of delegated legislation from parliamentary oversight: Final report (16 March 2021).

5 Schedule 1, item 5.

6 Schedule 1, item 5, proposed subsections 196A(7)–(8) set out the kinds of requirements that may be specified.

7 Schedule 1, item 5, proposed subsection 196A(5).

8 Schedule 1, item 5, proposed subsection 196A(5).

9 Schedule 1, item 5, proposed subsections 196A(9)–(10). At the time of writing, it was proposed that the value of the penalty unit be increased from $222 to $275. See Crimes Amendment (Penalty Unit) Bill 2022. Were this bill to pass, the applicable penalty would be $33,000.

10 Schedule 1, item 5, proposed subsection 196A(8), Note 1.

Summary of initial assessment

Preliminary international human rights legal advice

Right to health

2.6 To the extent that the measure prevents a disease or pest that may pose a risk to human health entering, establishing itself or spreading in Australian territory, it would promote the right to health. The right to health is the right to enjoy the highest attainable standard of physical and mental health, and requires States parties to take steps to prevent, treat and control epidemic diseases.[11]

Rights to privacy, freedom of movement, liberty and equality and non-discrimination

2.7 However, the measure would also engage and limit other human rights. Insofar as the measure may require individuals to provide a declaration containing certain information, including personal information, it would engage and limit the right to informational privacy. This is acknowledged in the statement of compatibility, which notes that the requirements may incidentally require individuals to provide personal information.[12] The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information, and the right to control the dissemination of information about one's private life.[13] Additionally, were a determination to require an individual to be screened by equipment or in any other physical way, and subjected to a biosecurity assessment involving a body or other physical search, the measure may engage and limit the right to personal autonomy and physical and psychological integrity – an aspect of the right to privacy.[14] The United Nations (UN) Human Rights Committee has emphasised that personal and body searches must be accompanied by effective measures to ensure that such searches are carried out in a manner consistent with the dignity of the person who is being searched, and further that persons subject to body searches should only be examined by persons of the same sex.[15]

2.8 The measure may also engage and limit the rights to freedom of movement and liberty if an individual was required to move to a place at the landing place or port for a biosecurity risk assessment and was detained while undergoing that assessment. The statement of compatibility states that this requirement may have the effect of preventing a person from leaving the landing place or port, or confining their movement within that landing place or port, until the level of biosecurity risk

11 International Covenant on Economic, Social and Cultural Rights, article 12.

12 Statement of compatibility, p. 41.

13 International Covenant on Civil and Political Rights, article 17.

14 See, *MG v Germany*, UN Human Rights Committee Communication No. 1428/06 (2008) [10.1].

15 UN Human Rights Committee, *General Comment No.16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (1988), [8].

associated with the individual has been assessed, and acknowledges that this may be considered administrative detention.[16] The right to freedom of movement includes the right to move freely within a country for those who are lawfully in the country.[17] The right to freedom of movement is linked to the right to liberty—a person's movement across borders should not be unreasonably limited by the State.[18] The right to liberty prohibits the arbitrary and unlawful deprivation of liberty.[19] The notion of 'arbitrariness' includes elements of inappropriateness, injustice and lack of predictability. Accordingly, any detention must be lawful as well as reasonable, necessary and proportionate in all of the circumstances.[20]

2.9 Additionally, depending on the persons or class of persons to whom the determination is applied, the measure may engage and limit the right to equality and non-discrimination. This is acknowledged by the statement of compatibility.[21] This right provides that everyone is entitled to enjoy their rights without discrimination of any kind and that all people are equal before the law and entitled without discrimination to equal and non-discriminatory protection of the law.[22] The right to equality encompasses both 'direct' discrimination (where measures have a discriminatory intent) and 'indirect' discrimination (where measures have a

16 Statement of compatibility, p. 27.

17 International Covenant on Civil and Political Rights, article 12.

18 UN Human Rights Committee, *General Comment 27: Freedom of movement* (1999) [8]. The freedom to leave the territory of a State may not be made dependent on any specific purpose or on the period of time the individual chooses to stay outside the country. The right of the individual to determine the State of destination is part of the legal guarantee.

19 International Covenant on Civil and Political Rights, article 9. It is noted that, depending on the degree and intensity, a restriction on liberty, such as restricting a person's liberty of movement, may not necessarily constitute 'deprivation' of liberty for the purposes of engaging this right. See United Nations Human Rights Committee, *General Comment No.27: Article 12 (Freedom of Movement)* (1999) [7]. See also, *Celepli v Sweden*, UN Human Rights Committee, Communication No. 456/1991 (2 August 1994); *Amuur v. France,* European Court of Human Rights, Application Nos. 17/1995/523/609, (1996), [42]; and *Guzzardi v. Italy*, European Court of Human Rights, Application no. 7367/76, (1980) [92].

20 In relation to administrative detention, the UN Human Rights Committee has stated that administrative or security detention – that is, detention not in contemplation of prosecution on a criminal charge – 'presents severe risks of arbitrary deprivation of liberty', especially where there is no limit on the overall length of possible detention and there is a risk that detention may last longer than absolutely necessary. See UN Human Rights Committee, *General Comment 35: Liberty and security of person* (2014) [15].

21 Statement of compatibility, p. 47.

22 International Covenant on Civil and Political Rights, articles 2 and 26. Article 2(2) of the International Covenant on Economic, Social and Cultural Rights also prohibits discrimination specifically in relation to the human rights contained in the International Covenant on Economic, Social and Cultural Rights.

discriminatory effect on the enjoyment of rights).[23] While the measure itself is drafted in neutral terms, were it to be applied to a particular class of persons on the basis of a protected attribute such as nationality or place of residence, it may constitute indirect discrimination.

2.10 These rights may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

Committee's initial view

2.11 The committee considered further information was required to assess the human rights compatibility of the measure, and as such sought the minister's advice in relation to:

(a) whether certain persons with protected attributes (such as nationality or place of residence) will be disproportionately affected by the measure;

(b) in relation to proposed paragraph 196A(8)(f), what other methods (apart from equipment) may be used to screen an individual;

(c) in relation to proposed paragraph 196A(8)(g), what would a biosecurity risk assessment of an individual involve. For example, could an individual be subjected to a body search or required to provide a bodily sample;

(d) how long a person or class of persons may be subject to administrative detention and whether there is a maximum length of detention;

(e) the conditions of administration detention;

(f) which existing powers in the Biosecurity Act may be invoked in relation to a requirement for an individual to move to a place for the purpose of a biosecurity risk assessment;

(g) whether decisions made pursuant to a determination made under section 196A will be reviewable;

(h) whether any less rights restrictive alternatives were considered, and if so, why these were considered inappropriate; and

(i) whether the measure is accompanied by any other safeguards.

2.12 The full initial analysis is set out in *Report 6 of 2022*.

23 UN Human Rights Committee, *General Comment 18: Non-discrimination* (1989).

Minister's response[24]

2.13 The minister advised:

a) whether certain persons with protected attributes (such as nationality or place of residence) will be disproportionately affected by the measure;

Section 196A enables the Agriculture Minister to make a determination to require specified incoming travellers to meet specified entry requirements in order to prevent, or reduce the risk of a disease or pest that poses an unacceptable biosecurity risk entering, establishing itself or spreading in Australian territory.

This is a legitimate purpose as it is intended to protect Australia, its plant and animal health, its economy and environment. Further, before specifying each entry requirement in a determination, the Agriculture Minister must be satisfied that the requirement is appropriate and adapted to meet this legitimate purpose.

As such, entry requirements will be determined on the basis of scientific and technical expertise and advice, and will be aimed at managing biosecurity risks in the most appropriate and least restrictive manner for the stated purpose.

For example, all travellers on a specified incoming vessel or flight, who have travelled to an area of biosecurity concern or have been exposed to certain animal, plants, or contaminated environments in the country that the vessel or flight originated from may be required to comply with certain entry requirements in a determination. The basis for making such a determination would relate solely to managing the biosecurity risk associated with the arriving travellers.

Entry requirements in a determination will not be applied to a class of individuals on the basis of protected attributes or characteristics, such as nationality or place of residence. An individual whose nationality or place of residence is the same as the country that the vessel or flight originated from will not be disproportionately affected by the measure because the measure will be applicable to all individuals on the vessel or flight regardless of their nationality or place of residence.

b) in relation to proposed paragraph 196A(8)(f), what other methods (apart from equipment) may be used to screen an individual;

An individual may be required to provide a declaration of information that will enable assessment of biosecurity risk. This could include whether they have been in contact with farms, farm animals, or wilderness areas that

24 The minister's response to the committee's inquiries was received on 19 January 2023. This is an extract of the response. The response is available in full on the committee's website.

are associated with biosecurity risk, or their intended activities whilst in Australia.

While the types of requirements that may be included in a determination made under section 196A that relate to screening are limited by safeguards (set out below), they are non-exhaustive so that different screening methods can be designed and appropriately tailored to respond to new and emerging biosecurity risks in the future. This will allow the legislative framework to keep pace with evolving biosecurity risks and enable the government to respond to these risks efficiently and effectively.

Screening of any kind must be for the purposes for which the determination had been made - that is, for the purposes of preventing, or reducing the risk of, the disease or pest to which the determination relates, entering, or establishing itself or spreading in, Australian territory or a part of Australian territory. Further, before specifying each entry requirement in a determination (including any requirement related to screening and any declaration related to screening), I or my duly authorised delegate must be satisfied that the requirement is appropriate and adapted to meet the stated purpose. As such, any screening requirement would be based on scientific and technical expertise and advice.

c) *in relation to proposed paragraph 196(8)(g), what would a biosecurity risk assessment of an individual involve. For example, could an individual be subjected to a body search or required to provide a bodily sample;*

Section 196(8)(g) does not authorise the taking of bodily samples or any other invasive procedure. Rather, a determination made under section 196A may include a requirement for an individual to attend a specific place within a landing place or port where they have arrived such as a client services desk to allow for an assessment of biosecurity risk. An assessment could include, for example, a biosecurity officer requiring an individual to provide verification that equipment used on animals has been appropriately sterilised and answer questions for the purpose of assessing the level of biosecurity risk associated with the individual and their goods.

d) *how long a person or class of persons may be subject to administrative detention and whether there is a maximum length of detention;*

A determination made under section 196A may include a requirement for a person or class of persons to move to a place within a landing place or port where they have arrived to allow for an assessment of biosecurity risk of the individual and any goods they are bringing with them into Australian territory.

This requirement is aimed at ensuring that individuals and groups of individuals are moved to one location in order to carry our biosecurity risk assessments on those individuals and their goods. This would manage and contain any potential risk that may be detected as part of this process.

Such a process would strengthen the ability to manage potentially high biosecurity risks in a controlled and discrete area, which may be crucial to prevent the further spread of certain diseases or pests that pose considerable threats to Australia's biosecurity systems.

It is intended that the length of time a person or class of persons may be required to remain at a place should be no longer than is appropriate for biosecurity officer to assess and manage any biosecurity risk associated with a person or their goods to an acceptable level. Whilst this may cause mild inconvenience for some persons arriving in Australia, such as a minor delay in exiting an airport or port, it is justified given the significant and devastating impact on Australia and its unique biosecurity status that would occur should a disease or pest posing unacceptable biosecurity risk enter Australia.

Where a determination is made under section 196A, the Agriculture Minister must be satisfied that any specified requirement is in relation to a disease or pest which poses an unacceptable level of biosecurity risk and the requirement is appropriate and adapted to prevent, or reduce the risk of, the pest or disease entering, or establishing itself or spreading in, Australian territory or a part of Australian territory. This means that each requirement must serve a legitimate purpose and must be necessary to meet that purpose. Where the above requirements are no longer met, the Agriculture Minister must vary or revoke the determination.

This will ensure that any determination made under section 196 and any specified requirements for persons to move to a place to be assessed for biosecurity risk will allow for a proportionate response based on scientific and technical advice, expertise and data.

e) the conditions of administrative detention;

If a determination were made under section 196A which included a requirement for individuals or classes of individuals to move to a place within a landing place or port where they have arrived to allow for an assessment of biosecurity risk, the location where such assessments would take place would vary on a case-by-case basis. It is anticipated that the location would be within the landing place or port where the travellers arrive in Australia, so the facilities and amenities typically associated with these places would be available. Biosecurity officials would interact with individuals on a case-by-case basis.

f) which existing powers in the Biosecurity Act may be invoked in relation to a requirement for an individual to move to a place for the purpose of a biosecurity risk assessment;

There are no existing powers in the Act that may be invoked to require a person or class of persons to move to a place for the purpose of a biosecurity risk assessment.

There is a power under section 60(1) of the Act which enables a chief human biosecurity officer, human biosecurity officer or biosecurity officer

to impose a human biosecurity control order (HBCO) on an individual for the purposes of managing any human health risk of a listed human disease that may be associated with the individual. The measures that may be included in a HBCO include measures that may require an individual to go to, and remain at, a specified premises, such as a medical facility, for the purposes of assessing or managing human health risk in relation to a listed human disease.

A HBCO that includes any measure that may require an individual to move to, and remain at, a specified premises for the purposes of assessing or managing human biosecurity risk may be imposed by a chief human biosecurity officer or human biosecurity officer, but not a biosecurity officer.

g) whether decisions made pursuant to a determination made under section 196A will be reviewable;

The types of requirements which may be included in a determination made under section 196A are set out in subsection 196A(8). The nature of these requirements are such that individuals to whom specified requirements apply will be required to comply with them upon arrival in Australia and while they are at the relevant landing place or port. It is anticipated that complying with specified requirements will therefore be completed before individuals leave the landing place or port at which they arrived.

Additionally, these requirements are of a preliminary nature. In effect, they allow information to be gathered from individuals arriving in Australia so that biosecurity risk may be more readily and accurately assessed. Depending on the information provided and the concomitant assessment, biosecurity officers may then make further decisions as to substantive treatment options.

Given the preliminary, information-gathering nature of the entry requirements and the anticipated short duration for an individual to comply with a requirement, it was considered unnecessary to subject this framework to a merits review process.

This does not, however, affect a person's right to seek judicial review in relation to the exercise of power in making an entry requirement determination. There is nothing to limit access to the courts or access to judicial review. Avenues to challenge executive decision-making remain.

h) whether any less rights restrictive alternatives were considered, and if so, why these were considered inappropriate;

The framework in the Bill is considered to be the most robust framework to manage the multiple biosecurity risks, both existing and emerging, that face Australia whilst giving due consideration to the impact that this may have on individual rights.

Australian businesses, individuals and global trading partners rely upon Australia's favourable biosecurity status and the Commonwealth's ability to effectively manage biosecurity risk in a timely manner. Where there is an imminent threat or actual outbreak of such disease or pest entering Australia, emergency action would be required to ensure fast and urgent action is taken to manage a threat or harm from the spread of the disease or pest within Australian territory.

A determination made under subsection 196A(2) would play a crucial role in that response and will be fundamental in the effective management of disease and may need to be made on a time critical basis to protect our industry and economy. The provision supports greater certainty for impacted industries, the individuals that implement these decisions and the broader community in order to protect Australia's plant and animal health, the nation's $70 billion dollar agriculture industry and the 1.6 million jobs that rely on it.

Notably, the provisions in Schedule 1 contain a number of legislative safeguards to reasonably constrain the exercise of power under sections 196A and 196B. These safeguards lessen the impact the provisions may have on individuals and are discussed below.

i) whether the measure is accompanied by any other safeguards;

The measures include a number of safeguards which constrain the powers to make determinations under section 196A. For example, each entry requirement in a determination must be appropriate and adapted to its purpose. That purpose is expressly set out in subsection 196A(1) – that is, preventing or reducing the risk of a disease or pest that poses an unacceptable biosecurity risk entering, establishing itself or spreading in Australian territory. The assessment of whether entry requirements in a determination are appropriate and adapted is informed, structured and underpinned by scientific and technical processes, data and expertise. This means that the impact the requirements may have on individuals and their rights only goes so far as is required to satisfy the scientific and technical advice in order to determine requirements that prevent or reduce the risk of a disease or pest entering, establishing itself or spreading in Australia.

Further, the provisions include additional protections to ensure that a determination made under section 196A is only in place for the minimum time that it is needed. For example, proposed subsection 196B(1) requires that, in relation to a determination made under proposed subsection 196A(2), the Agriculture Minister must vary or revoke such a determination if satisfied that the relevant disease or pest no longer poses an unacceptable biosecurity risk or that a requirement is no longer appropriate and adapted for its purpose. This effectively acts as a constraint on the Agriculture Minister's exercise of power as it compels variation or revocation if a pest no longer poses a risk or a requirement is no longer appropriate and adapted. This means that individuals will only

be impacted by such a determination for the time needed to meet the relevant biosecurity risk.

Lastly, subsection 196A(9) requires the Agriculture Minister, before making the determination, to consult with the Director of Biosecurity, the Director of Human Biosecurity and the head of the State or Territory body that is responsible for the administration of matters relating to biosecurity in each State and Territory. Such consultation provides a further valuable safeguard.

Concluding comments

International human rights legal advice

Rights to health, privacy, freedom of movement, liberty and equality and non-discrimination

2.14 As outlined above, while the measure could promote the right to health to the extent that it prevents a disease or pest that may pose a risk to human health entering, establishing itself or spreading in Australian territory, it would also engage and limit the rights to privacy, freedom of movement, liberty and, depending on the persons or class of persons to whom the determination is applied, equality and non-discrimination. As to the latter, the minister advised that the entry requirements will be determined on the basis of scientific and technical expertise and advice, not on the basis of protected attributes or characteristics, such as nationality or place of residence. While it is acknowledged that the measure is drafted in neutral terms and an entry requirement may not be applied specifically on the basis of nationality or place of residence, given the nature of the measure, there appears to remain a risk that in practice a determination could have a disproportionate impact on certain nationalities (noting it may apply to passengers arriving from select countries, with more of the passengers likely to be nationals of that country) such that it may constitute indirect discrimination. Differential treatment (including the differential effect of a measure that is neutral on its face) will not constitute unlawful discrimination if the differential treatment is based on reasonable and objective criteria such that it serves a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.[25]

2.15 As noted in the initial analysis, the measure pursues the legitimate objective of preventing the entry and spread of pests and diseases, and imposing entry requirements that assist to identify and manage such risks would likely be effective to achieve this objective. The key question, applicable to assessing the compatibility of the measure with the right to equality and non-discrimination and the rights to privacy, freedom of movement and liberty, is whether the limitations are proportionate to this stated objective. The initial analysis noted a number of

25 UN Human Rights Committee, *General Comment 18: Non-Discrimination* (1989) [13]; see also *Althammer v Austria*, UN Human Rights Committee Communication No. 998/01 (2003) [10.2].

safeguards that would likely assist with proportionality, including the requirements that the minister be satisfied of certain things before making a determination and must revoke or vary the determination if they are no longer satisfied of these things.[26] The requirement that the minister consult with certain people and bodies before making a determination may also operate as a safeguard, although its strength is lessened by the fact that a failure to comply with this consultation requirement does not affect the validity of the determination.[27] Regarding other safeguards, the minister stated that each entry requirement in a determination must be appropriate and adapted to its purpose, and informed, structured and underpinned by scientific and technical processes, data and expertise.

2.16 While these requirements appear to go some way to ensuring that any interference with rights is only as extensive as is strictly necessary, questions remain as to whether these safeguards will be sufficient in practice, noting that much will depend on the specific determination and the breadth of its operation. In this regard, it is relevant to consider how the measure will operate in practice, particularly the processes surrounding biosecurity risk assessments and associated administrative detention.

2.17 In relation to what other methods (apart from equipment and the provision of a declaration) may be used to screen an individual for the purposes of a biosecurity risk assessment, the minister advised that the types of screening methods are non-exhaustive so that different screening methods can be designed and appropriately tailored to respond to new and emerging biosecurity risks in the future. The minister stated that screening of any kind must be for the purposes for which the determination has been made and the entry requirement itself must be appropriate and adapted to meet the stated purpose. The minister further advised that the measure does not authorise the taking of bodily samples or any other invasive procedure for the purposes of a biosecurity risk assessment. Rather, an assessment could include a biosecurity officer requiring an individual to provide verification that equipment used on animals has been appropriately sterilised and answer questions about themselves and their goods. Based on this further information, it appears that a requirement for an individual to be screened and subject to a biosecurity risk assessment under this measure would not involve invasive personal procedures or other physical searches. This assists with proportionality, particularly in relation to any potential limitation on the right to

26 Schedule 1, item 5, proposed subsection 196A(5) and section 196B.

27 Schedule 1, item 5, proposed subsections 196A(9) and (10).

personal autonomy and physical and psychological integrity – an aspect of the right to privacy.[28]

2.18 Additionally, further information was sought regarding the length of any detention when a person is required to move to a certain place for the purposes of a biosecurity risk assessment, as well as the conditions of detention and whether there is access to review. These factors are relevant considerations in assessing whether administrative detention in the context of this measure constitutes arbitrary deprivation of liberty such that it constitutes an impermissible limit on the right to liberty. International human rights law jurisprudence has indicated that detention that may initially be necessary and reasonable may become arbitrary over time if the circumstances no longer require detention. In this respect, regular review must be available to scrutinise whether the continued detention is lawful and non-arbitrary. In the context of administrative detention, the UN Human Rights Committee has stated that States parties 'need to show that detention does not last longer than absolutely necessary, that the overall length of possible detention is limited and that they fully respect the guarantees provided for by article 9 in all cases'.[29]

2.19 The minister advised that the intended length of time a person may be required to remain at a place should be no longer than is appropriate for biosecurity officers to assess and manage any biosecurity risk associated with the person or their goods. The minister stated that whilst this may cause mild inconvenience or minor delays, it is justified given the significant and devastating impact on Australia and its unique biosecurity status were a disease or pest to enter Australia. The minister noted that conducting biosecurity risk assessments in one location would strengthen the ability to manage potentially high biosecurity risks in a controlled and discrete area. As to the conditions of detention, the minister advised that the location where such assessments will take place will vary on a case-by-case basis, but it is anticipated that the location will be within a landing place or port where travellers arrive in Australia, so the associated facilities and amenities in those locations would be available.

2.20 Regarding the availability of review, the minister advised that given the preliminary, information-gathering nature of the entry requirements and the anticipated short duration for an individual to comply with a requirement, it was considered unnecessary to subject this framework to a merits review process.

---

28 See, *MG v Germany*, UN Human Rights Committee Communication No. 1428/06 (2008) [10.1]. While an individual may not be subject to invasive procedures or treatment under this bill, they may be subject to such procedures or treatment under existing powers in the Biosecurity Act. For example, an individual could be subject to a human biosecurity control order under subsection 60(1), which may require an individual to move to, and remain at, a specified premises, such as a medical facility, for the purposes of assessing or managing human biosecurity risk.

29 UN Human Rights Committee, *General Comment 35: Liberty and security of person* (2014) [15].

However, judicial review remains available as an avenue to challenge the exercise of power in making an entry requirement determination.

2.21 While it is intended that this power would be used for short durations, without a maximum length of detention or other legislative safeguard to ensure that any detention does not last longer than is absolutely necessary, and without access to merits review, there appears to be some risk that administrative detention in the context of this measure could be arbitrary in practice, depending on the length and conditions of such detention. As to whether any limitations on other human rights will be proportionate in practice, much will depend on the specific requirements contained in any determination and the consequent extent of any interference with rights. For example, were a determination to require a person to provide a declaration containing personal information, be screened by equipment and move to, and be detained at, a landing place for the purpose of a biosecurity risk assessment, the cumulative impact of these requirements may result in greater interference with rights. In general, the greater the interference, the less likely the measure is to be considered proportionate. As such, noting the breadth of entry requirement that could be made, there appears to be some risk that the powers could be used in a way that may be incompatible with human rights.

Committee view

2.22 The committee thanks the minister for this response. The committee considers that empowering the Agriculture Minister to make entry requirements for people entering Australia in order to prevent the entry or spread of diseases or pests that pose a risk to human health, promotes the right to health. However, the committee notes that requiring people to provide personal information, be screened, or moved to locations to carry out biosecurity risk assessments, also engages and may limit the rights to privacy, freedom of movement and liberty and the right to equality and non-discrimination (were it to have a disproportionate impact on persons from particular countries).

2.23 The committee considers that the measure pursues the legitimate objective of preventing the entry and spread of pests and diseases in Australia and is accompanied by some important safeguards that assist with proportionality. Based on the information provided by the minister, it appears that, in many cases, the use of these determinations would constitute a proportionate limitation on human rights. However, the committee notes that given the breadth of the measure, there remains a risk that the powers could be used in a way that may not be compatible with human rights. In particular, the committee notes that in relation to any administrative detention under this measure, there is no maximum length of detention or other legislative safeguard to ensure that any detention does not last longer than is necessary, as well as no access to merits review. In the absence of these safeguards, there may be a risk that were an individual to be detained for the purpose of a biosecurity risk assessment for longer than is absolutely necessary, such administrative detention may be considered arbitrary in practice. Regarding

potential limitations on other human rights, the committee notes that the proportionality of such limitations will depend on the specific requirements contained in any determination and the consequent extent of any interference with rights.

2.24 As the bill has now passed, the committee makes no further comment on this bill.

Preventative biosecurity measures

2.25 The bill also seeks to confer new powers on the Agriculture Minister to determine, by exempt legislative instrument,[30] certain other biosecurity measures for the purposes of preventing a specified behaviour or practice that causes or contributes to the entry into, or the emergence, establishment or spread in, Australian territory of a specified disease (other than a listed human disease) or pest that is considered to pose an unacceptable level of biosecurity risk.[31] The determination would apply to specified classes of persons and may ban or restrict, or require, a behaviour or practice; require the provision of a specified report; or provide for tests to be conducted on goods or conveyances.[32]

2.26 Before making a preventative biosecurity measure, the minister must be satisfied that the disease or pest poses an unacceptable level of biosecurity risk; and the measure is appropriate and adapted to prevent, or reduce the risk of, the disease or pest entering, or establishing itself or spreading in, Australian territory or part of Australian territory.[33] The minister would also be required to consult with certain persons, including the Directors of Biosecurity and Human Biosecurity, before making a determination, although failure to do so would not affect the validity of the determination.[34] Additionally, failure to comply with a preventative biosecurity measure would attract a civil penalty of 120 penalty units (currently $26,640).[35]

30 Schedule 1, item 11, proposed subsection 393B(4) provides that a determination made under this section is a legislative instrument but the disallowance provision (section 42 of the *Legislation Act 2003*) does not apply to the instrument.

31 Schedule 1, item 11.

32 Schedule 1, item 11, proposed subsection 393B(2).

33 Schedule 1, item 11, proposed subsection 393B(5).

34 Schedule 1, item 11, proposed subsection 393B(5).

35 Schedule 1, item 11, proposed subsections 393B(7)–(8).

Summary of initial assessment

Preliminary international human rights legal advice

Right to health

2.27 To the extent that the determination could prevent a behaviour or practice that causes the entry, establishment or spread of a disease or pest in Australian territory that may pose a risk to human health, it may promote the right to health.

Rights to privacy, equality and non-discrimination, culture, and freedom of movement

2.28 However, the measure would also engage and limit other human rights. By banning, restricting or requiring a behaviour or practice, and requiring a person to provide a specified report or keep specified records, the measure would engage and limit the right to privacy.[36] Further, depending on the class of persons to whom the determination is applied, the measure may engage and limit the right to equality and non-discrimination, as acknowledged by the statement of compatibility.[37] Additionally, depending on the content of the determination, including the behaviour or practice that is restricted or banned, the measure may engage other human rights. For example, were the determination to ban or restrict traditional trading practices in the Torres Strait Islands, it may engage and limit the right to culture[38]—which, in the context of Indigenous peoples, includes the right to use land resources including through traditional activities such as hunting and fishing, and to live on their traditional lands—as well as related rights under the United Nations Declaration on the Rights of Indigenous Peoples.[39] It could also engage and limit the right to freedom of movement if the behaviours to be restricted include prohibiting movement to particular locations.

2.29 The above rights may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

36 International Covenant on Civil and Political Rights, article 17.

37 Statement of compatibility, p. 47.

38 International Covenant on Economic, Social and Cultural Rights, article 15; and International Covenant on Civil and Political Rights, article 27. See also, UN Committee on Economic, Social and Cultural Rights, *General Comment No. 21: article 15 (right of everyone to take part in cultural life)* (2009). The committee explains, at [6], that the right requires from a State party both abstention (including non-interference with the exercise of cultural practices) and positive action (including ensuring preconditions for participation, facilitation and promotion of cultural life).

39 See, eg, United Nations Declaration on the Rights of Indigenous Peoples, article 8 (right not to be subjected to forced assimilation or destruction of their culture) and 11 (right to practise and revitalize cultural traditions and customs).

Committee's initial view

2.30 The committee considered further information was required to assess the human rights compatibility of this measure, and as such sought the minister's advice in relation to:

(a) whether certain persons with protected attributes (such as nationality or place of residence) will be disproportionately affected by the measure;

(b) what types of behaviours and practices would likely be specified in a determination, and in particular, is it likely that a determination would ban or restrict:

(i) traditional trading or other cultural practices among Aboriginal and Torres Strait Islander persons, particularly in the Torres Strait Islands;

(ii) movement between particular locations;

(c) whether decisions made pursuant to a determination made under section 393B will be reviewable;

(d) whether any less rights restrictive alternatives were considered, and if so, why these were considered inappropriate; and

(e) whether the measure is accompanied by any other safeguards

The full initial analysis is set out in *Report 6 of 2022*.

Minister's response[40]

2.31 The minister advised:

a) whether certain persons with protected attributes (such as nationality or place of residence) will be disproportionately affected by the measure;

Section 393B enables the Agriculture Minister to make a determination that specifies any one or more of the following biosecurity measures to be taken by specified classes of persons:

a. banning or restricting a behaviour or practice

b. requiring a behaviour or practice

c. requiring a specified person to provide a specified report or keep specified records

d. conducting specific tests on specified goods or specified conveyances.

40 The minister's response to the committee's inquiries was received on 19 January 2023. This is an extract of the response. The response is available in full on the committee's website.

A biosecurity measure must not be specified in a determination unless the Agriculture Minister is satisfied that a disease or pest poses an unacceptable level of biosecurity risk and the measure is appropriate and adapted to prevent, or reduce the risk of, the pest or disease entering, or emerging, or establishing itself or spreading in, Australian territory or a part of Australian territory.

As such, biosecurity measures will be determined on the basis of scientific and technical expertise and advice, and will be aimed at managing biosecurity risks in the most appropriate and least restrictive manner for the stated purpose.

For example, all travellers on a specified incoming vessel or flight, who have travelled to an area of biosecurity concern or have been exposed to certain animal, plants or contaminated environments in the country that the vessel or flight originated from may be required to comply with certain biosecurity measures in a determination. The basis for making such a determination would relate solely to managing the biosecurity risk associated with the arriving travellers.

Biosecurity measures in a determination will not be applied to a specified classes of persons on the basis of protected attributes or characteristics, such as nationality or place of residence. An individual whose nationality or place of residence is the same as the country that the vessel or flight originated from will not be disproportionately affected by the measure because the measure will be applicable to all individuals on the vessel or flight regardless of their nationality or place of residence.

b) what types of behaviours and practices would likely be specified in a determination, and in particular, is it likely that a determination would ban or restrict:

(i) traditional trading or other cultural practices among Aboriginal and Torres Strait Islander persons, particularly in the Torres Strait Islands;

(ii) movement between particular locations;

The types of biosecurity measures, including the types of behaviours and practices, that may be included in a determination made under section 393B will vary from case to case and will depend on a number of factors such as the type of disease or pest and treatment methods available to manage the relevant biosecurity risks. For example, a behaviour or practice which may be included in a determination would be walking over a foot mat at a landing place or port that contains a solution to treat fabric and surfaces should this be considered appropriate and adapted for the purposes of addressing the relevant biosecurity risk.

All biosecurity measures specified in a determination must be appropriate and adapted to prevent, or reduce the risk of, the pest or disease entering, emerging, establishing itself or spreading in, Australian territory or a part of Australian territory. For example, a measure that requires the treatment

of goods would require the treatment to be appropriately tailored to the pest or disease that poses an unacceptable level of biosecurity risk and suitable for application by a biosecurity officer or treatment provider.

It is not the policy intention to include requirements in a determination made under section 393B that would ban or restrict traditional trading or other cultural practices among Aboriginal and Torres Strait Islander persons.

Depending on various factors discussed below, it may be necessary to restrict movement between particular locations to reduce the spread of a pest or disease, and effectively and appropriately manage the associated biosecurity risk. Assessing whether such a restriction would be necessary would involve consideration of a range of factors which may be specific to a location such as the pest or disease status, facilities available to manage biosecurity risk, activities being undertaken, environmental conditions and susceptible plants and animal species present. As noted above, however, any such biosecurity measures that did so restrict movement would be informed, structured and underpinned by scientific and technical processes, data and expertise in order to ensure that the measure was appropriate and adapted to meet the purpose of preventing, or reducing the risk of, the pest or disease entering, emerging, establishing itself or spreading in, Australian territory or a part of Australian territory.

c) whether decisions made pursuant to a determination made under section 393B will be reviewable;

As noted above, an anticipated type of biosecurity measure that may form part of a determination made under section 393B would include requiring travellers to walk over a foot mat at a landing place or port upon arrival in Australia. Given the anticipated duration that an individual needs to comply with such a biosecurity measures it was considered unnecessary to subject this framework to a merits review process.

This does not, however, affect a person's right to seek judicial review in relation to the exercise of power in making a determination under section 393B. There is nothing to limit access to the courts or access to judicial review. Avenues to challenge executive decision-making remain.

d) whether any less rights restrictive alternatives were considered, and if so, why these were considered inappropriate; and

The framework in the Bill is considered to be the most robust framework to manage the multiple biosecurity risks, both existing and emerging, that face Australia whilst giving due consideration to the impact that this may have on individual rights.

Australian businesses, individuals and global trading partners rely upon Australia's favourable biosecurity status and the Commonwealth's ability to effectively manage biosecurity risk in a timely manner. Where there is an imminent threat or actual outbreak of such disease or pest entering Australia, emergency action would be required to ensure fast and urgent

action is taken to manage a threat or harm from the spread of the disease or pest within Australian territory. A determination made under subsection 393B(2) will play a crucial role in that response and will be fundamental in the effective management of disease and may need to be made on a time critical basis to protect our industry and economy. The provision supports greater certainty for impacted industries, the individuals that implement these decisions and the broader community in order to protect Australia's plant and animal health, the nation's $70 billion dollar agriculture industry and the 1.6 million jobs that rely on it.

Notably, the provisions contain a number of legislative safeguards to reasonably constrain the exercise of power under section 393B. These safeguards lessen the impact the provisions may have on individuals and lessen the impact they may have on individuals. These are discussed below.

e) whether the measure is accompanied by any other safeguards.

The measures include a number of safeguards, which constrain the powers to make determinations under section 393B. For example, each biosecurity measure in a determination must be appropriate and adapted to its purpose. That purpose is expressly set out in subsection 393B(1) – that is, preventing or reducing the risk of a disease or pest that poses an unacceptable biosecurity risk entering, or emerging, or establishing itself or spreading in Australian territory. The assessment of whether biosecurity measures in a determination are appropriate and adapted is informed, structured and underpinned by scientific and technical processes, data and expertise. This means that the impact the requirements may have on individuals and their rights only goes so far as is required to satisfy the scientific and technical advice in order to determine requirements that prevent or reduce the risk of a disease or pest entering, emerging, establishing itself or spreading in Australia.

Further, the provisions include additional protections to ensure that a determination made under section 393B is only in place for a limited time. Subsection 393B(5) limits the duration of such a determination to one year, but it would nevertheless remain possible to vary or revoke a determination before a year has passed, if the relevant risk no longer exists. This acts as a constraint on the Agriculture Minister's exercise of power. This means that individuals will only be impacted by such a determination for the time needed to meet the relevant biosecurity risk, with a maximum period of effect of one year.

Lastly, subsection 393BA(7) requires the Agriculture Minister, before making the determination, to consult with the Director of Biosecurity, the Director of Human Biosecurity and the head of the State or Territory body that is responsible for the administration of matters relating to biosecurity in each State and Territory. Such consultation provides a further valuable safeguard.

Concluding comments

International human rights legal advice

Rights to health, privacy, equality and non-discrimination, culture, and freedom of movement

2.32 As outlined above, while the measure could promote the right to health to the extent that it prevents a disease or pest that may pose a risk to human health entering, establishing itself or spreading in Australian territory, it would also engage and limit the rights to privacy and equality and non-discrimination, depending on the class of persons to whom the determination is applied. In relation to the right to equality and non-discrimination, the minister advised that the entry requirements will be determined on the basis of scientific and technical expertise and advice, not on the basis of protected attributes or characteristics, such as nationality or place of residence. As noted above, while the measure is drafted in neutral terms and an entry requirement may not be applied specifically on the basis of nationality or place of residence, given the nature of the measure, there appears to remain a risk that in practice a determination could have a disproportionate impact on certain nationalities such that it may constitute indirect discrimination (noting that differential treatment, including the differential effect of a measure that is neutral on its face, will not constitute unlawful discrimination if the differential treatment is based on reasonable and objective criteria).

2.33 Additionally, depending on the content of the determination, including the behaviour or practice that is restricted or banned, the measure may engage other human rights, such as the rights to culture and freedom of movement. Further information was sought from the minister in this regard to fully assess what human rights are likely to be engaged by the measure. The minister advised that the types of behaviours and practices that may be included in a determination will vary from case to case and will depend on several factors, such as the type of disease or pest and the available treatment methods. For example, a practice that may be required would be walking over a foot mat at a landing place or port that contains a solution to treat fabric and surfaces. The minister stated that it is not the policy intention to include a requirement that bans or restricts traditional trading or other cultural practices among Aboriginal and Torres Strait Islander persons. However, a determination may restrict movement between particular locations to reduce the spread of a pest or disease. The minister noted that any such biosecurity measures that restricted movement would be informed, structured and underpinned by scientific and technical processes, data and expertise to ensure the measure was appropriate and adapted to meet its stated purpose.

2.34 While it is acknowledged that the measure is not intended to ban traditional trading or other cultural practices, it may nevertheless have this effect if doing so were considered necessary to reduce the spread of a pest or disease and the measure was appropriate and adapted to prevent or reduce this risk. As such,

depending on how the measure is used in practice, it appears it could engage and limit the right to freedom of movement and the right to culture.

2.35 In assessing the compatibility of the measure with the above rights, the initial analysis noted that the stated objective of the measure – namely, to prevent a behaviour or practice that may cause or contribute to a disease or pest, that poses an unacceptable level of biosecurity risk, entering, emerging, establishing or spreading in Australian territory[41] – would be legitimate for the purposes of international human rights law. Further, preventing such behaviours or practices would likely be effective to achieve this objective. The key question remaining is whether the proposed limitations on rights are likely to be proportionate.

2.36 In considering whether the measure is sufficiently circumscribed, the initial analysis noted that there are some requirements that assist to clarify the scope of the minister's powers and provide some guidance as to how the powers may be exercised. For example, the measure requires the minister to specify the behaviour or practice and the disease or pest to which the determination would apply; be satisfied of specific things; and consult with specific people before making a determination.[42] However, there remains some uncertainty as to the types of behaviours or practices that may be specified in a determination, noting the minister's advice that the behaviours or practices to be included in a determination will vary from case to case and depend on a number of factors.

2.37 International human rights law jurisprudence states that laws conferring discretion or rule-making powers on the executive must indicate with sufficient clarity the scope of any such power or discretion conferred on competent authorities and the manner of its exercise.[43] This is because, without sufficient safeguards, broad powers may be exercised in such a way as to be incompatible with human rights. While there may be some risk that this could occur given the breadth of the powers contained in the measure, much will depend on how the powers are exercised in practice.

2.38 Another safeguard in the bill is the requirement that the determination must not be in force for more than one year. On this point, the minister advised that while the determination is limited to one year, there remains the possibility of the determination being varied or revoked earlier if the relevant risk no longer exists. The minister stated that this acts as a constraint on the minister's exercise of power as individuals will only be impacted by a determination for the time needed to meet the relevant biosecurity risk, with a maximum period of one year. As to the availability of review of decisions made pursuant to a determination, the minister stated that merits review is not available and was not considered necessary given the

41 Schedule 1, item 11, proposed section 393A and subsection 393B(1).

42 Schedule 1, item 11, proposed subsections 393B(3) and (5).

43 *Hasan and Chaush v Bulgaria,* European Court of Human Rights App No.30985/96 (2000) [84].

anticipated duration that an individual needs to comply with such a biosecurity measure. While it is anticipated that it will be a short duration in which an individual will be required to comply with a biosecurity measure, such as a requirement to walk over a foot mat at a landing place, the legislation allows for the determination to be in force for one year. This may constitute a substantial period of time depending on the extent of interference with rights. For example, were a determination to ban certain trading practices or restrict movement between particular locations for the duration of one year, it may represent a substantial interference with rights. Further, while judicial review remains available, this is a more limited form of review than merits review, only allowing a court to consider whether the decision to make the determination was lawful (and not allowing it to consider the merits of making the determination).

2.39 In conclusion, while the measure is accompanied by some safeguards, given the breadth of the measure and noting there is no limit on the types of behaviours or practices that may be specified in a determination and the lack of merits review, there appears to be a risk that, depending on the nature of the determination, the measure may not constitute a proportionate limit on rights in practice.

Committee view

2.40 The committee thanks the minister for this response. The committee considers that empowering the Agriculture Minister to determine certain biosecurity measures, for the purposes of preventing a specified behaviour or practice that causes or contributes to the entry or spread into Australia of certain diseases or pests that may pose a risk to human health, promotes the right to health. However, the committee notes that banning, restricting, or requiring certain behaviours or practices or requiring the provision of specified information also engages and may limit other human rights, including the rights to privacy, equality and non-discrimination, culture and freedom of movement.

2.41 The committee considers the measure pursues the legitimate objective of preventing a behaviour or practice that may cause or contribute to a disease or pest, that poses an unacceptable level of biosecurity risk, entering, emerging, establishing or spreading in Australian territory. While the measure is accompanied by some important safeguards, the committee notes the measure empowers the making of a relatively broad determination to prohibit variable types of behaviours and practices. The committee notes that, in many cases, the types of behaviours or practices required will represent a proportionate limit on rights, such as a requirement that individuals walk over a foot mat at a landing place. However, given the breadth and flexibility of the power, there remains a risk that, depending on the nature of the determination, the existing safeguards may not be sufficient in practice to safeguard rights.

2.42 As the bill has now passed, the committee makes no further comment on this bill.

Information management framework

2.43 Schedule 3 to the bill seeks to amend the Biosecurity Act in relation to the management of information obtained or generated under the Act, in particular to enable greater sharing of information with government agencies and other bodies.

2.44 In particular, Schedule 3 seeks to introduce the concept of 'entrusted persons' who would have specific authorisations to deal with 'relevant information'.[44] The information that it applies to would include personal information, some of which may be obtained using the coercive powers under the Biosecurity Act (such as the powers referenced above).

2.45 An 'entrusted person' is defined in the bill[45] as meaning relevant Commonwealth ministers or departmental secretaries or the Director of Biosecurity or the Director of Human Biosecurity, as well as:

- any Australian Public Service (APS) employee in the Agriculture Department or the Health Department;
- anyone employed or engaged to provide services to the Commonwealth in connection with the Agriculture Department or the Health Department; or
- anyone employed or engaged by the Commonwealth or a statutory body corporate that is in a prescribed class of persons (with the class to be prescribed in future regulations).

2.46 The bill provides that entrusted persons would then be authorised to deal with the information in a variety of ways, including:

- disclosing the information to a state or territory body, or foreign government, in order to manage risks posed by diseases and pests;[46]
- disclosing the information to a court or tribunal for the purposes of law enforcement or to assist in the review an administrative decision;[47]
- disclosing information for the purpose of enforcing the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue, to a body that enforces such laws (including the police);[48] and

44 Schedule 3, item 8 defines 'relevant information' to mean information obtained or generated by a person in the course of, or for the purposes of, performing functions or duties or exercising powers under the Biosecurity Act, or assisting another person to do this.

45 See Schedule 3, item 5, definition of 'entrusted person'.

46 Schedule 3, item 27, proposed sections 584 and 585.

47 Schedule 3, item 27, proposed section 588.

48 Schedule 3, item 27, proposed section 589.

- using or disclosing the information for research, policy development or data analysis or statistics.[49]

2.47 In addition, relevant information would be authorised to be disclosed in the course of, or for the purposes of, performing functions or duties, or exercising powers, under the Biosecurity Act, or assisting another person to do so.[50] The persons that could disclose information for this purpose would include:

- entrusted persons;
- persons employed or engaged by the Commonwealth or a statutory body corporate;
- various biosecurity officials;
- biosecurity industry participants or their employees (which carry out specified activities to manage the biosecurity risks associated with imported goods);[51] and
- survey authorities or their officers or employees (which appear to be international shipping authorities).[52]

2.48 The bill does not set out who the information could be disclosed to. There would also be a separate authorisation for certain persons to use or disclose relevant information for the purposes of managing risks to human health.[53] Such persons would include entrusted persons, persons employed or engaged by the Commonwealth or a body corporate established by Commonwealth law, biosecurity officials, chief human biosecurity officers, human biosecurity officers and biosecurity industry participants (including their officers or employees).

49 Schedule 3, item 27, proposed sections 590 and 590A.

50 Schedule 3, item 27, proposed section 582.

51 *Biosecurity Act 2015*, sections 9 and 14 defines a 'biosecurity industry participant' as being the holder of the approval of an approved arrangement.

52 *Biosecurity Act 2015*, section 9 defines 'survey authority' as meaning a person authorised by the Director of Biosecurity under section 290A to be a survey authority. Section 290A allows persons to be prescribed to meet ballast water functions, and the Biosecurity (Ballast Water Survey Authority) Authorisation (No. 2) 2017 authorises the following: American Bureau of Shipping (ABS); Bureau Veritas (BV); Det Norske Veritas Germanischer Lloyd (DNV GL); Lloyd's Register (LR); Nippon Kaiji Kyokai (Class NK); China Classification Society (CCS); Korean Register of Shipping (KR); Registro Italiano Navale (RINA).

53 Schedule 3, item 27, proposed section 583.

Summary of initial assessment

Preliminary international human rights legal advice

Right to privacy

2.49 By authorising the use and disclosure of personal information, the measure would engage and limit the right to privacy.[54] This is acknowledged in the statement of compatibility.[55] The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, the measure must pursue a legitimate objective and be rationally connected to (that is, effective to achieve) and proportionate to achieving that objective.

Committee's initial view

2.50 The committee considered further information was required to assess the human rights compatibility of this measure, and as such sought the minister's advice in relation to:

a) the person or body to whom relevant information may be disclosed for the purposes of the Biosecurity Act (proposed section 582) or other Acts (proposed section 586) and managing human health risks (proposed section 583)—noting that in these circumstances, it is not clear to whom the information may be disclosed;

b) why it is necessary to allow all information obtained using powers under the Biosecurity Act to be shared for law enforcement purposes, unrelated to managing biosecurity risks or the administration of the Biosecurity Act;

c) why an information sharing agreement is not required in relation to all circumstances where personal information is shared between the Commonwealth and another entity or body; and

d) what other safeguards accompany the measure to protect personal information. For example, is there a requirement that personal information be stored on a secure database or destroyed after a set amount of time.

2.51 The full initial analysis is set out in *Report 6 of 2022*.

54 International Covenant on Civil and Political Rights, article 17.

55 Statement of compatibility, p. 44.

Minister's response[56]

2.52 The minister advised:

I acknowledge the committee's concern around measures which may engage and limit the right to privacy and address these in detail below including the safeguards in place to protect personal information.

a) the person or body to whom relevant information may be disclosed for the purposes of the Act (s.582) or other Acts (proposed s.586) and managing human health risks (s.583) – noting that it is not clear to whom the information may be disclosed

Section 582 authorises the use or disclosure of relevant information for the purposes of performing functions or duties, or exercising powers, under the Act, or assisting another person to do the same, without limiting to whom any such disclosures may be made. The disclosure of information is governed and limited by the functions, duties and powers under the Act and other under relevant legislation such as the *Privacy Act 1988*. For example, when a biosecurity officer gives a person in charge of an aircraft or vessel a direction in relation to the unloading of goods (see section 143 of the Act), then the authorisation under section 582 would allow the biosecurity officer to disclose relevant information to the person in charge that is for the purposes of exercising the power to issue a direction.

A further limitation is that relevant information may only be disclosed under sections 582, 583 or 586 for the specified legislative purpose under which they operate, including the Act, other Acts or for managing human health risks. For example, in section 583, the purposes are clearly confined to those relating to one of the specific risks or emergencies listed in subsection 583(1), all of which relate to managing human health risks. The purposes set out in section 586 relate to the administration of the Act or other Acts administered by the Agriculture Minister or the Health Minister. This authorisation by definition limits the persons to whom disclosure of relevant information is allowed as there must be a clear nexus between the disclosure and the specific human health purpose or legislative purpose of the relevant Act.

Subdivision A would therefore confine disclosure to persons who would legitimately require the information in order to achieve and manage one of the listed purposes in the relevant legislation. As risks may emerge suddenly, without warning and in an unexpected or novel form, it is appropriate to frame the disclosure authorisations in sections 582, 583, and 586 in such a way as to provide maximum flexibility to respond to what may be urgent human health and biosecurity risks as they arise as well as to routine matters under the Act. Further, recipients of relevant

56 The minister's response to the committee's inquiries was received on 19 January 2023. This is an extract of the response. The response is available in full on the committee's website.

information will be governed by other legislative frameworks in relation to what they can then do with such information. For example, if information is provided to a person exercising powers and functions under the *Export Control Act 2020* then the information will be governed by that statute. If information is provided to a State or Territory body, then the information will be governed by State or Territory laws.

In relation to protected information, there are sanctions for unauthorised use or disclosure. The offence in subsection 580(6) is triggered if certain persons who obtained or generated protected information in the course of, or for the purposes of, performing functions or duties, or exercising powers, under the Act (or assisting another person to perform such functions or duties, or exercise such powers), use or disclose protected information, and the use or disclosure is not required or authorised by a Commonwealth law or a prescribed State or Territory law (and where the good faith exception in subsection 580(4) does not apply).

b) why it is necessary to allow all information obtained using powers under the Act to be shared for law enforcement purposes, unrelated to managing biosecurity risks or the administration of the Act.

The amendments are intended to reflect best practice by streamlining information sharing, including for the purposes of law enforcement. Section 589 authorises disclosure for the purposes of law enforcement to certain Commonwealth, State or Territory bodies which have a law enforcement or protection of public revenue function. Relevant law enforcement purposes may include the investigation of offences under the *Crimes Act 1914*. This amendment is also consistent with the way information sharing regimes are framed in other legislation, for example the *Hazardous Waste (Regulation of Exports and Imports) Act 1989* and the *Industrial Chemicals Act 2019*.

Authorised purposes include the administration of state/territory laws (section 590F) and where this may not necessarily be limited to biosecurity purposes, the disclosure of information to a State or Territory body would need to be governed by an agreement between the Commonwealth and the State or Territory body.

A robust and effective framework for information sharing for law enforcement, governed by clear guidelines and responsibilities, is necessary to protect Australia's public interest. The amendments address a number of identified shortcomings with the previous arrangements for information sharing under the Act including the need to simplify and clarify the regime, and allow a key element of best practice, that is, the ability to share information for law enforcement purposes. Instead of providing for exceptions to offence provisions, the amendments provide for a single set of positive authorisations, including for law enforcement. At times the initial stages of law enforcement investigations are by their nature undefined and need to be sufficiently wide-ranging to allow the proper

investigation of differing, intersecting issues before an effective enforcement decision can be made.

The enforcement of Australian laws is an appropriate framing for the authorised disclosure of relevant information, as it is a matter of public interest. I consider that there are sufficient checks and balances on the use of such information and the authorisation allows the Commonwealth to make a judgement about the necessity of sharing for any proposed purpose.

c) *why an information sharing agreement is not required in relation to all circumstances where personal information is shared between the Commonwealth and another entity or body.*

Information sharing agreements are initiated on a case-by-case basis, taking into account the circumstances and merits of each proposed agreement. Information sharing agreements, particularly those which occur on a regular basis, may be appropriate, for example for the purposes of law enforcement because of the potentially serious consequences for the outcome of certain law enforcement actions. There may be other circumstances, such as research, policy development or data analysis or statistics, where it may also be appropriate to govern information sharing via an agreement.

In some circumstances it may be neither practical nor possible to enter into information sharing agreements. For example, in emergency situations it may not be feasible to have an agreement before the Commonwealth shares information about a highly infectious disease under section 582 of the Act. It may be necessary to disclose to certain members of the community that there is a new infectious human disease, in a situation where some personal information also needs to be disclosed. The personal information may be about the age/gender of person (relevant to the epidemiology of the disease), or information about their movements (for contract tracing purposes) and it would not be feasible to enter agreements with each member of the community.

The Department of Agriculure [sic], Fisheries and Forestry currently has information sharing agreements with other agencies and New Zealand governing sharing of information, criteria, procedures and privacy management and mitigation strategies. Existing arrangements will be reviewed to ensure compliance with the new framework.

d) *what other safeguards accompany the measure to protect personal information, for example, is there a requirement that personal information be stored on a secured database or destroyed after a set amount of time*.

The department maintains robust policies and procedures to protect any personal information which it holds, as documented in the department's Privacy Policy at agriculture.gov.au/about/commitment/privacy.

Personal information is held in accordance with the collection and security requirements of the Australian Privacy Principles, the department 's policies and procedures and the Australian Government Protective Security Policy Framework (AGPSPF). The department holds personal information in a range of audio-visual, paper and electronic based records (including in cloud-based applications and services). The department complies with the AGPSPF for protecting departmental resources (including information) from harm or unauthorised access.

If personal information held by the department is lost, or subject to unauthorised access or disclosure, the department will respond in accordance with the Office of the Australian Information Commissioner's guidelines.

Relevant departmental policies and procedures, which can be implemented on a case-by-case basis, include the following:

- application of additional restrictions, including via protective marking, to limit the clearance level for access of personal information
- requiring agreement of affected parties for any particular disclosure or use
- ensuring the storage of personal information meets best practice protocols; and
- requiring the mandatory destruction of the personal information after an agreed timeframe and in an agreed manner.

Concluding comments

International human rights legal advice

Right to privacy

2.53 To assess whether the proposed limitation on the right to privacy is proportionate, further information was sought regarding the breadth of the measure, particularly in relation to the persons to whom, and the bases on which, information may be disclosed under the information management framework. While the measure mostly provides for who may use the relevant information (namely, an entrusted person), and the persons to whom information may be disclosed, there are some circumstances where this is not the case.[57] In particular, sections 582, 583 and 586 authorise the disclosure of relevant information for specified purposes without limiting to whom any such disclosures may be made. The minister advised that disclosure of information under these sections is governed and limited by the functions, duties and powers under the Act and other relevant legislation such as the *Privacy Act 1988* as well as the fact that disclosure must be for the specified

57 See Schedule 3, item 27, proposed sections 582, 583 and 586.

legislative purpose under which it operates. The effect of this would be to confine disclosure to persons who would legitimately require the information to achieve and manage one of the listed purposes in the relevant legislation. The minister considered that it is appropriate to frame the disclosure authorisations in sections 582, 583 and 596 in such a way as to provide maximum flexibility to respond to what may be urgent human health and biosecurity risks as they arise as well as routine matters under the Act. The minister further noted that recipients of relevant information under these sections will be governed by other legislation, such as state and territory laws if the recipient was a state or territory body.

2.54 It is noted that sections 582, 583 and 586 place limitations regarding the persons who are authorised to disclose relevant information (namely, entrusted persons) and the purposes for which information may be disclosed, which could, as the minister suggests, have the effect of limiting the persons to whom information may be disclosed. However, without limiting to whom information may be disclosed in the text of the legislation itself, it remains unclear how broadly this power would be exercised. For example, in the case of disclosing information for the purpose of managing a human biosecurity emergency, it appears possible that information could be disclosed to a broad range of front line workers, private companies and contractors, such as airport staff and transport workers. In order to be proportionate, a limitation on the right to privacy should only be as extensive as is strictly necessary and legislation must specify in detail the precise circumstances in which interferences with privacy may be permitted.[58]

2.55 As to the bases on which information may be disclosed, further information was sought as to why it is necessary to allow all information obtained using powers under the Act to be shared for law enforcement purposes, unrelated to managing biosecurity risks or the administration of the Act (as permitted under section 589). The minister advised that the amendments are intended to reflect best practice by streamlining information sharing, including for the purposes of law enforcement. The minister stated that a robust and effective framework for information sharing for law enforcement, governed by clear guidelines and responsibilities, is necessary to protect Australia's public interest. The minister noted that initial stages of law enforcement investigations are, by their nature, undefined and need to be sufficiently wide-ranging to allow the proper investigation of differing, intersecting issues before an effective enforcement decision can be made.

2.56 However, questions remain as to whether sharing all information obtained by officials using powers under the Biosecurity Act to enforce any other law, unrelated to any biosecurity risk or for the administration of the Biosecurity Act, will be proportionate in practice, noting that the adequacy of the public interest justification will depend on the circumstances of each case. Given the breadth of this information-sharing power and the corresponding considerable extent of the

58 *NK v Netherlands*, UN Human Rights Committee Communication No.2326/2013 (2018) [9.5].

potential interference with the right to privacy, it is critical that the measure is accompanied by stringent safeguards to ensure any limitation on the right to privacy is proportionate.

2.57 In this regard, the initial analysis identified some safeguards that would assist with proportionality, including:

- requiring reasonable steps to be taken to de-identify personal information in the context of information used or disclosed for research, policy development or data analysis (but not other purposes);[59]
- permitting the use or disclosure of relevant information that is statistical information that is not likely to enable the identification of a person;[60]
- requiring an agreement to be in place between the Commonwealth and a state or territory body before the relevant information may be disclosed to the body. The agreement may include a requirement that the state or territory body confirm any personal information disclosed is subject to appropriate safeguards;[61]
- the discretion of the Commonwealth to make an information sharing agreement or impose conditions on the use or disclosure of relevant information shared under this division;[62] and
- the prohibition on unauthorised use or disclosure of protected information.[63]

2.58 Regarding information sharing agreements, the minister advised that these agreements are initiated on a case-by-case basis, taking into account the circumstances and merits of each proposed agreement. The minister noted that an information sharing agreement may be appropriate in a law enforcement or research, policy development or data analysis context, but in other circumstances may neither be practical nor possible, such as in an emergency situation.

2.59 As to the existence of other safeguards, the minister referred to the department's Privacy Policy and the Australian Government Protective Security Policy Framework. The minister further noted that certain departmental policies and

59 Schedule 3, item 27, proposed section 590; statement of compatibility, pp. 44–45.

60 Schedule 3, item 27, proposed section 590A; statement of compatibility, p. 45.

61 Schedule 3, item 27, proposed sections 589 and 590F; statement of compatibility, p. 45.

62 Schedule 3, item 16, proposed section 579, Note 2 provides that nothing in Part 2 of Chapter 11 of the Biosecurity Act would prevent the Commonwealth from making agreements or other arrangements to impose conditions on the use or disclosure of relevant information by a body or person who obtains the information as a result of an authorised disclosure.

63 Schedule 3, item 18, proposed section 580, which would apply a fault-based offence, civil penalty provision and strict liability offence to the unauthorised use or disclosure of protected information which is obtained or generated under the Biosecurity Act.

procedures can be applied on a case-by-case basis, such as requiring the mandatory destruction of personal information after an agreed timeframe and in an agreed manner or applying additional restrictions to limit the clearance level for access to personal information.

2.60 The above safeguards would assist with proportionality, although it is noted that discretionary safeguards are less stringent than the protection of statutory processes as there is no requirement to follow them. However, given the breadth of the measure, including the absence of a limit on the persons to whom information may be disclosed in certain circumstances and the type of information that may be shared for law enforcement purposes, there is a risk that the existing safeguards may not be adequate in all circumstances so as to ensure that any limitation on the right to privacy will be proportionate in practice.

Committee view

2.61 The committee thanks the minister for this response. The committee considers that authorising the use and disclosure of personal information engages and limits the right to privacy.

2.62 The committee considers that the measure pursues the legitimate objective of supporting the management of biosecurity risks and facilitating the effective operation and enforcement of the Biosecurity Act. The committee considers that the measure is accompanied by a number of important safeguards that will help to ensure any interference with the right to privacy is only as extensive as is strictly necessary. However, given the breadth of the measure, there is a risk that the existing safeguards may not be adequate in all circumstances so as to ensure that any limitation on the right to privacy will be proportionate in practice.

2.63 As the bill has now passed, the committee makes no further comment on this bill.

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022[1]

Purpose	This bill (now an Act) enhances the protection of personal information by increasing penalties, strengthening the Australian Information Commissioner's (the Commissioner) enforcement powers, and providing the Commissioner and Australian Communications and Media Authority (ACMA) with greater information sharing arrangements
Portfolio	Attorney-General
Introduced	House of Representatives, 27 October 2022 (received Royal Assent on 12 December 2022)
Rights	Privacy; criminal process rights

2.64 The committee requested a response from the minister in relation to the bill in *Report 6 of 2022*.[2]

Increasing civil penalties

2.65 The bill (now Act) amended the *Privacy Act 1988* (Privacy Act) to increase penalties under section 13G for serious or repeated interferences with the privacy of an individual.[3] Section 13G previously made it a civil penalty punishable by up to 2,000 penalty units (which was $444,000) if an entity does an act, or engages in a practice, that seriously interferes with the privacy of an individual or repeatedly interferes with the privacy of one or more individuals. The Act increased the maximum civil penalty for breach of this provision for 'a person other than a body corporate' to $2.5 million. It also significantly increased the penalty applicable to body corporates to up to $50 million.

Summary of initial assessment

Criminal process rights

2.66 The significant proposed increase in this civil penalty to a maximum of $2.5 million for persons other than a body corporate, to the extent that it applies to

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, *Report 1 of 2023*; [2023] AUPJCHR 11.

2 Parliamentary Joint Committee on Human Rights, *Report 6 of 2022* (24 November 2022), pp. 50-55.

3 Item 14.

individuals,[4] raises the risk that this penalty may be considered criminal in nature under international human rights law. Under Australian law, civil penalty provisions are dealt with in accordance with the rules and procedures that apply in relation to civil matters (the burden of proof is on the balance of probabilities). However, if the new civil penalties as applicable to individuals are regarded as 'criminal' for the purposes of international human rights law, they would engage the criminal process rights under articles 14 and 15 of the International Covenant on Civil and Political Rights, including the right not to be tried or punished twice[5] and the right to be presumed innocent until proven guilty according to law,[6] which requires that the case against the person be demonstrated on the criminal standard of proof of beyond reasonable doubt.

2.67 The test for whether a civil penalty should be characterised as 'criminal' for the purposes of international human rights law relies on three criteria:

(a) the domestic classification of the offence as civil or criminal;

(b) the nature of the penalty; and

(c) the severity of the penalty.[7]

2.68 As to the nature of the penalties and when the penalties may apply (whether to the public or in a regulatory or disciplinary context), section 13G operates with respect to 'entities', which means an agency, organisation or small business operator.[8] The Privacy Act defines an organisation or small business operator as including an individual.[9] The statement of compatibility states that the existing civil penalties in section 13G 'fall short of community expectations, particularly if it is large multinational organisations being penalised'.[10] However, it is not clear whether and how section 13G may operate with respect to individual persons who are not operating within a specific regulatory or disciplinary context. For example, would it apply to a naturopath, gym-owner or childcare operator who regularly emails their clients a newsletter and accidentally shares their client email addresses in doing so? In this regard, it is unclear whether the nature of conduct which could give rise to a

4 Noting that human rights apply only to humans, this advice does not consider the proposed increase in relation to bodies corporate.

5 International Covenant on Civil and Political Rights, article 14(7)

6 International Covenant on Civil and Political Rights, article 14(2).

7 For further detail, see the Parliamentary Joint Committee on Human Rights, *Guidance Note 2*: *Offence provisions, civil penalties and human rights* (December 2014).

8 *Privacy Act 1988*, section 6.

9 *Privacy Act 1988*, subsection 6C(1)(a) and section 6D. An 'agency' may likewise include a person, but only where they are holding or performing the duties of an appointment or office. See, *Privacy Act 1988*, section 6.

10 Statement of compatibility, p. 6.

serious or repeated interference with privacy would be such that penalties for breaches of section 13G would necessarily be restricted to specific regulatory contexts. The term 'serious interference' or 'repeated' is not defined in the Privacy Act,[11] and the explanatory materials accompanying this bill do not elucidate the circumstances which could give rise to a serious or repeated interference with privacy by a person other than a body corporate. There also appears to be limited jurisprudence interpreting section 13G to date. Consequently, some questions remain with respect to the nature of section 13G, and the circumstances in which it may apply. It seems possible that the section could apply beyond specific regulatory or disciplinary contexts and affect the public more generally.

2.69 A penalty is more likely to be considered criminal for the purposes of international human rights law if the penalty carries a term of imprisonment or a substantial pecuniary sanction. While the civil penalty provisions would not carry a term of imprisonment, the maximum penalty amount of $2.5 million for individuals is a substantial pecuniary sanction.

2.70 The full initial analysis is set out in *Report 6 of 2022*.

Committee's initial view

2.71 The committee noted that the objective of the bill is to strengthen protections against unlawful interferences with privacy,[12] and considered that this is an important objective. The committee therefore considered that, in general, these proposed information-sharing and enforcement powers would likely promote the right to privacy.

2.72 The committee noted that these proposed information-sharing and enforcement powers would also limit the right to privacy and the right to a fair hearing, including by compelling the provision of information or documents.[13]

2.73 In relation to those aspects of the bill seeking to increase to $2.5 million civil penalties applicable to individuals, the committee noted this may engage criminal process rights and sought the Attorney General's advice in relation to:

(a) examples of the type of individuals section 13G would apply to, and whether any individuals would be covered by the provision who may not fully understand the regulatory context (noting the examples in the advice above);

11 The explanatory material accompanying the bill which originally established section 13G of the Privacy Act (the Privacy Amendment (Enhancing Privacy Protection) Bill 2012) provides no further explanation of its intended scope of operation.

12 See, statement of compatibility, p. 4.

13 See, for example, items 38–41, which would establish civil penalties contraventions of the obligation to give information, answer a question or produce a record or document under the Privacy Act.

(b) examples of the types of conduct that may constitute a serious interference, and a repeated interference, with privacy under section 13G of the *Privacy Act 1988*, particularly with respect to conduct by individuals; and

(c) in those instances where an individual may be subject to a significant penalty under the proposed changes to section 13G, why requiring the courts to apply a higher civil standard of proof would not be appropriate.

Minister's response[14]

2.74 The minister advised:

> The Privacy Act applies to organisations with an annual turnover more than $3 million, subject to some exceptions. The Privacy Act defines an 'organisation' under section 6C of the Act, which can include an individual such as a sole trader. However, the Privacy Act does not generally apply to an individual acting in a personal capacity but more generally directed to a range of organisations including agencies, a body corporate or other entities.
>
> The Australian Government recognises it is important that organisations understand their obligations under the Privacy Act and that guidance is available. As part of its functions, the Australian Information Commissioner (Commissioner) is responsible for working with entities to help them understand their obligations and the regulatory context. This includes:
>
> - making guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals
> - promoting an understanding and acceptance of the Privacy Act, and
> - undertaking educational programs for the purposes of promoting the protection of individual privacy.
>
> The Office of the Australian Information Commissioner (OAIC) publishes detailed guidance and advice on its website, as well as training resources and is also able to undertake assessments of an organisation's compliance with the Privacy Act.
>
> Civil penalty orders would only be pursued for the most serious or repeated privacy breaches, and this is outlined in the OAIC's *Privacy regulatory action policy* guidance which notes:
>
> - The OAIC's privacy regulatory action would be proportionate to the situation or conduct concerned.

14 The minister's response to the committee's inquiries was received on 9 December 2022. This is an extract of the response. The response is available in full on the committee's website.

- The OAIC's preferred regulatory approach is to work with entities to facilitate legal and best practice compliance and that it can use a range of steps as part of this approach, only some of which involve the use of regulatory powers.

In relation to civil penalties proposed under the Bill, I note the following:

1. they are not classified as 'criminal' under Australia law;
2. they are intended to be a strong deterrent against serious or repeated privacy breaches, but do not apply to individuals at large - only individuals that are 'organisations' under the Privacy Act may be subject to the penalties (for example, sole traders that have more than $3 million in annual revenue); and
3. they do not carry a penalty of imprisonment, and provide for substantial financial penalties to be imposed by a court in relation in the most serious or repeated privacy breaches.

On this basis, the Government considers it is appropriate and proportionate to apply the civil standard of proof in the circumstances where an individual will only be liable to the penalties in section 13G when the individual is an 'organisation' for the purposes of the Privacy Act (that is, generally where they are not acting in a personal capacity), and the threshold for a serious or repeated interference with privacy is high and reserved for the most egregious breaches. While the maximum penalty is being raised, the court retains discretion on determining penalties, and will only apply maximum penalties to appropriate cases taking into account all relevant matters. This will include factors such as the nature and extent of the contravening conduct, the damage or loss suffered, the size of the contravening entity and whether the entity has previously been found to have engaged in similar conduct.

While the Government is acting now to increase penalties under section 13G, I also note that the Attorney-General's Department's review of the Privacy Act (the Review) is considering whether the civil penalty provision for a serious or repeated interference with privacy under section 13G could be made clearer. For example, the legislation could specify those types of factors the OAIC currently considers relevant in its guidance which could include circumstances where the information is highly sensitive, there has been wilful misconduct, or it adversely affects large groups of individuals. Further, the Review is considering whether the current spectrum of regulatory options available are too limited to target the different levels of seriousness with which interferences with privacy occur, and whether it would appropriate to have tiered penalty provisions. A lower tiered penalty may be appropriate in circumstances where the conduct is not a serious or repeated breach of privacy, but enforcement action is still warranted.

Concluding comments

International human rights legal advice

2.75 In relation to the types of individuals who may be regulated by the Privacy Act, and so subject to the operation of section 13G, the Attorney-General advised that the Act will only apply to individuals where they are operating as sole traders and their organisation's annual turnover exceeds $3 million. The Attorney-General stated that the Privacy Act does 'not generally apply to an individual acting in a personal capacity'. That is, 'an individual will only be liable to the penalties in section 13G when the individual is an 'organisation' for the purposes of the Privacy Act (that is, generally where they are not acting in a personal capacity)'. It would appear, therefore, that section 13G is unlikely to operate in relation to individuals, and not in relation to the public at large, but only in a particular regulatory context, where individuals should understand the obligations they owe.

2.76 The Attorney-General also stated that the government considers it is appropriate and proportionate to apply the civil standard of proof in the circumstances, and noted that the court retains discretion on determining penalties, and will only apply maximum penalties to appropriate cases taking into account all relevant matters (which will include: the nature and extent of the contravening conduct; the damage or loss suffered; the size of the contravening entity; and whether the entity has previously been found to have engaged in similar conduct). In addition, the Attorney-General noted that his department is currently considering whether the civil penalty provision for a serious or repeated interference with privacy under section 13G could be made clearer, including whether the legislation could specify relevant factors, such as in 'circumstances where the information is highly sensitive, there has been wilful misconduct, or it adversely affects large groups of individuals'. The explicit inclusion of such matters would appear capable of guiding the application of the potential penalty under section 13G, such that the maximum potential penalty is only available in the most serious cases. Further, having regard to the Attorney-General's advice as to the applicability of the penalty to individuals only in a regulatory context, it appears that the penalty is unlikely to engage criminal process rights under international human rights law.

Committee view

2.77 The committee thanks the Attorney-General for this response. The committee considers, based on this advice, that these amendments to significantly increase civil penalties for serious or repeated interferences with privacy, are unlikely to engage criminal process rights under international human rights law, noting the limited applicability of these penalties to individuals. The committee considers that its concerns have therefore been addressed, and makes no further comment in relation to this bill.

Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022[1]

Purpose	This bill seeks to amend the *Telecommunications Act 1997* to alter the operation of information disclosure provisions and record of disclosure requirements. It would also make technical amendments to the *Telstra Corporation and Other Legislation Amendment Act 2021*
Portfolio	Infrastructure, Transport, Regional Development, Communications and the Arts
Introduced	House of Representatives, 10 November 2022
Rights	Privacy; effective remedy

2.78 The committee requested a response from the minister in relation to the bill in *Report 6 of 2022*.[2]

Increased access to the Integrated Public Number Database

2.79 The bill seeks to amend the *Telecommunications Act 1997* (Telecommunications Act) to expand the information that may be disclosed from the Integrated Public Number Database (Number Database), allowing disclosure of information related to unlisted (and listed) phone numbers in the case of calls to emergency services numbers.[3] It would also insert a requirement that it must be unreasonable or impracticable to obtain the other person's consent to the disclosure or use of their information.

Summary of initial assessment

Preliminary international human rights legal advice

Right to privacy

2.80 Permitting the use and disclosure of personal information related to unlisted phone numbers on the Number Database in emergency call situations engages and limits the right to privacy. The right to privacy may be subject to permissible

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022, *Report 1 of 2023*; [2023] AUPJCHR 12.

2 Parliamentary Joint Committee on Human Rights, *Report 6 of 2022* (24 November 2022), pp. 56-67.

3 Items 1–6. See, *Telecommunications Act 1997,* section 285.

limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, the measure must pursue a legitimate objective and be rationally connected to (that is, effective to achieve) and proportionate to achieving that objective.

2.81 Permitting the disclosure of unlisted phone numbers in such circumstances in order to protect life is a legitimate objective for the purposes of international human rights law, and this measure appears to be rationally connected to (that is, capable of achieving) that objective. But questions remain regarding proportionality.

Committee's initial view

2.82 While noting the important objective of this bill, the committee noted that permitting the disclosure of information relating to unlisted phone numbers (such as mobile phone numbers) on the Integrated Public Number Database in dealing with matters raised by a call to an emergency service number engages and limits the right to privacy and sought the minister's advice as to:

(a) whom information or documents obtained under this measure may be disclosed, and examples of such disclosure;

(b) what are the parameters of the term 'dealing with matters raised by' a call to an emergency service number;

(c) whether and how the alternative basis for disclosing information relating to a call to an emergency services phone number in section 286 interacts with this proposed amendment to section 285, and why the proposed amendment is necessary despite this existing exception; and

(d) what safeguards would apply to information disclosed under section 285 as amended (including restrictions in terms of how the data must be handled, used, stored, and destroyed).

2.10 The full initial analysis is set out in *Report 6 of 2022*.

Minister's response[4]

2.83 The minister advised:

> **(a) To whom may information obtained under this measure be disclosed, with examples of disclosure?**
>
> The Bill facilitates the disclosure of information about unlisted numbers from the Manager of the Integrated Public Number Database (IPND) to the Emergency Call Person.

4 The minister's response to the committee's inquiries was received on 9 December 2022. This is an extract of the response. The response is available in full on the committee's website.

In practice, the information is disclosed to emergency services (police, fire or ambulance). When a caller dials an emergency service number in need of emergency assistance, the call is first answered by the Emergency Call Person (currently Telstra for 000/112, and the National Relay Service provider for 106). The Emergency Call Person asks the caller which emergency service is required – police, fire, or ambulance – and then connects the caller to the relevant emergency service centre that services the caller's location[5].

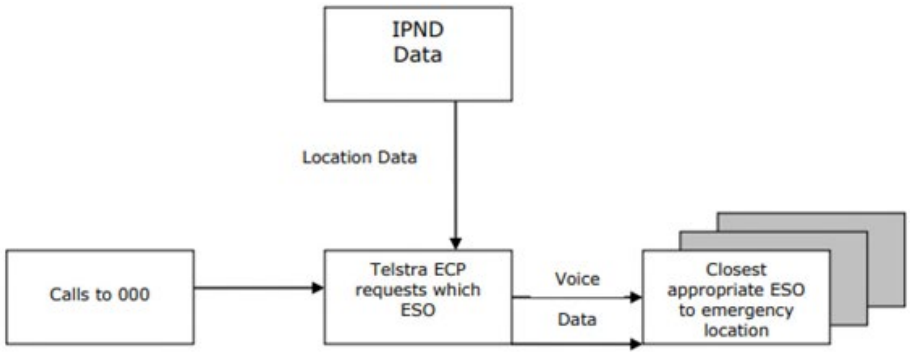

Figure 1: An overview of what happens on an emergency call

When the call is transferred to the requested emergency service, the customer name and residential address of the caller is automatically transmitted from the IPND and displayed on the control screen of the emergency service operator handling the call. In most cases, the operator is able to confirm the appropriate dispatch location directly with the caller.

However, if this location cannot be confirmed, assistance is dispatched to the address associated with the phone number of the caller, as listed on the IPND. The IPND, which is managed by Telstra under clause 10 of its carrier license conditions,[6] contains a record of each telephone number issued by carriage service providers to their customers in Australia, including the customer's name and residential address. Access to information in the IPND – including storage, transfer, use, or disclosure of unlisted information – is strictly regulated through the Act, a number of legislative instruments, and enforceable industry standards. Further information is provided under response (c).

The proposed amendment to section 285 of the Act is mainly focused at promoting clarity in the legislative framework around the disclosure of unlisted number information. As set out in paragraph 13 of the *Notes on*

5 Page 14 of the IPND Data G619:2017 Communications Alliance Industry Guideline outline the processes relating to emergency service calls, including how information derived from the IPND is used for the purpose of emergency call services.

6 See: Telecommunications (Carrier Licence Conditions - Telstra Corporation Limited) Declaration 2019

Clauses in the Explanatory Memorandum for the Bill, the intention is to remove unnecessary complexity in the interpretation of the Act – however, the proposed measure also introduces an additional safeguard that it must be unreasonable or impracticable to seek the consent of the person to whom the disclosure relates.

(b) What are the parameters of 'dealing with matters raised by' a call to an emergency service number?

Disclosure of unlisted information through the proposed measure will be limited in practice to dispatching services (such as an ambulance) and routing calls to either Triple Zero or the Australian 106 Text Emergency Relay Service for people who have a hearing or speech impairment. In law, they are strictly limited to matters raised by a call to an emergency service number.

(c) Does the alternative basis for disclosing information relating to a call to an emergency services phone number in section 286 interact with this proposed amendment to section 285, and if so, how? Why is the proposed amendment necessary despite this existing exception?

No. The exception in section 286 only applies to information that is known or comes into a person's possession because of a call to an emergency service number. It allows the Emergency Call Person to disclose information to the appropriate ESO. It does not extend to the IPND Manager (i.e. information in the IPND does not come into possession of the IPND Manger as a result of a call to an emergency number).

The exception in section 285, and the proposed amendment, applies in a different circumstance and is also narrower. It applies only to information contained in the IPND, only to the Manager of the IPND, and only for purposes of dealing with a matter raised by a call to an emergency service number. The proposed amendment merely clarifies that disclosure about unlisted numbers from the IPND Manager to the Emergency Call Person (for example, to allow the dispatch of an ambulance because the person on the call using an unlisted number is asphyxiating) is lawful.

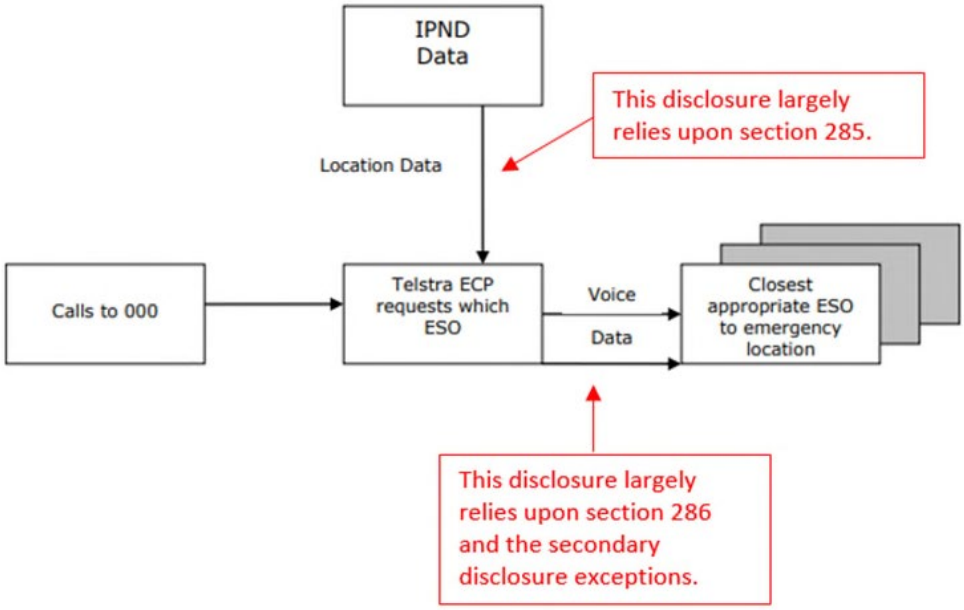

Figure 2: an overview of which provisions apply to which disclosure

(d) What are the safeguards that would apply to information disclosed under section 285 as amended (including restrictions in terms of how the data must be handled, used, stored, and destroyed)?

The amendment builds upon the existing Part 13 safeguards by introducing a requirement that it must be unreasonable or impracticable to seek the consent of the person to whom the disclosure relates. The use and disclosure of this data is restricted only to those necessary in providing an emergency service response. Through the interaction between several pieces of legislation which regulate either access to information in the IPND and/or the provision of emergency call services, information disclosure through the measure is restricted to police, fire and ambulance services.

Beyond this, the general safeguards that apply across Part 13 of the Act remain in place. For example, Division 2 of the Act sets out that use or disclosure of information received under these exceptions must be for the authorised purpose, contravention of which is an offence punishable on conviction by 2 years imprisonment, for example.

Telstra, as the IPND Manager and the Emergency Call Person (ECP), has publicly available procedures in place to ensure that information disclosed between the IPND Manager and the ECP is handled appropriately.[7] Obligations on IPND access seekers are specified in an enforceable

7 Part 8 of the Telecommunications (Consumer Protection and Service Standards) Act 1999 and the Telecommunications (Emergency Call Service) Determination 2019 set out obligations relating to the provision of emergency call services, including call information.

industry code[8] and in the data access agreements with Telstra.[9] These technical implementations limit the ability for disclosures to occur for purposes or to entities separate to those mentioned above.

Concluding comments

International human rights legal advice

Right to privacy

2.84 As to whom information or documents obtained under this measure may be disclosed, the minister advised that information is disclosed to emergency services (police, fire or ambulance). When a caller dials an emergency service number, the call is answered by the Emergency Call Person who asks the caller which emergency service is required and then connects the caller to the relevant emergency service centre that services the caller's location. Following the transfer of the call, the caller's name and residential address is automatically transmitted from the Number Database and displayed on the control screen of the emergency service operator handling the call. Consequently, it appears that information or documents obtained under this measure may only be disclosed to emergency services workers.

2.85 In relation to the parameters of 'dealing with matters raised by' a call to an emergency service number, the minister advised that this will be limited in practice to dispatching services (such as an ambulance) and routing calls to either Triple Zero or the Australian 106 Text Emergency Relay Service for people who have a hearing or speech impairment. It would appear, therefore that this provision only operates in respect of immediate responses to calls made to emergency services (and not, for example, to permit disclosure at some later time).

2.86 The minister further advised that this provision is necessary, because existing provisions in the Telecommunications Act (including section 286) operate differently to this proposed amendment. The minister advised that the exception in section 286 only applies to information that is known or comes into a person's possession because of a call to an emergency service number, allowing the Emergency Call Person to disclose information to the appropriate Emergency Services Officer. Section 285 (as amended), by contrast, would apply in different and more narrow circumstances: to information contained on the Number Database, to be relied on by the Number Database Manager, and only for purposes of dealing with a matter raised by a call to an emergency service number (for example, to allow the dispatch of an ambulance because the person on the call using an unlisted number is

8 See: Integrated Public Number Database C555:2020 (industry code registered under Part 6 of the Act)

9 For example, Data Users and Data Providers Technical Requirements for IPND outlines technical requirements of the IPND, including for file formatting and storage, data security, and reporting. IPND homepage link: https://www.telstra.com.au/consumer-advice/ipnd

asphyxiating). Based on this additional information, it is clear that sections 285 and 286 facilitate the disclosure of information to different workers where an emergency phone call has been made, and therefore operate differently.

2.87 The minister also outlined several safeguards which would apply to information disclosed under section 285 as amended. The minister noted the proposed inclusion of an additional safeguard by introducing a requirement that it must be unreasonable or impracticable to seek the consent of the person to whom the disclosure relates. In addition, the minister noted there is already: an offence to use or disclose information received under these exceptions other than for the authorised purpose; procedures that govern how Telstra, as the Number Database Manager and the Emergency Call Person, must handle information appropriately; as well as obligations on those seeking access to the Number Database via an enforceable industry code and in data access agreements with Telstra. These safeguards assist with the proportionality of the measure.

2.88 Based on this additional information from the minister, it would appear that the power under section 285 (as amended) is appropriately circumscribed and accompanied by valuable safeguards such that it is likely to constitute a proportionate limitation on the right to privacy.

Committee view

2.89 The committee thanks the minister for their comprehensive response to its questions about this measure, and considers that based on this additional information, allowing disclosure of information related to unlisted (and listed) phone numbers, in the case of calls to emergency services numbers, would likely constitute a proportionate limit on the right to privacy. The committee welcomes the minister's advice that the explanatory materials accompanying this bill will be updated to reflect this additional information.

Sharing of information in the case of a threat to a person's life or health

2.90 The bill seeks to expand a further exception from the use and disclosure offences set out in Part 13 of the Telecommunications Act where the disclosure relates to threats to a person's life or health.[10] Section 287 currently provides that a person may disclose or use information or a document relating to the affairs or personal particulars (including any unlisted telephone number or any address) of another person if the first person 'believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person'. The bill seeks to remove the qualifier that a threat to

10 Items 7–8 amending section 287.

the life or health of a person be 'imminent' and insert a requirement that it is unreasonable or impracticable to obtain the other person's consent to the disclosure or use of information.

2.91 The bill also seeks to repeal and replace section 300, which provides for the secondary use and disclosure of information that has been obtained under section 287.[11] This would allow for the secondary disclosure or use of information by the person who obtained it from the carriage service provider or carrier where it is unreasonable or impracticable to obtain consent and either: the disclosure or use is for the purpose of, or in connection with, preventing or lessening a serious threat to the life or health of a person; or the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious threat to the life or health of a person.

Summary of initial assessment

Preliminary international human rights legal advice

Right to privacy

2.92 The proposed expansion of the exception from the use and disclosure offences set out in Part 13 of the Telecommunications Act where the disclosure relates to threats to a person's life or health engages and limits the right to privacy. The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, the measure must pursue a legitimate objective and be rationally connected to (that is, effective to achieve) and proportionate to achieving that objective.

2.93 Permitting the disclosure of information (and its onward disclosure) in order to protect life and health of a person is a legitimate objective, and this measure appears to be rationally connected to (that is, capable of achieving) that objective. However, with respect to the proportionality of the measure, the statement of compatibility does not outline whether the measure is appropriately circumscribed and fails to identify any safeguards relating to access to, and the use of, such data.

Committee's initial view

2.94 The committee considered further information was required to assess the compatibility of the measure with the right to privacy, and sought the minister's advice as to:

(a) what is the process by which section 287 is invoked (for example, is it only ever police contacting carriage service providers in practice?), and is a warrant or other formal application a part of the process;

11 Item 9.

(b) what specific kinds of information may be used or disclosed as a result of the offence provisions not applying. In particular, would it allow for the content of a person's text messages or voicemail or their call log to be made available, or only the GPS phone triangulation;

(c) how such data is managed on receipt, and whether, how, and for how long such data is then stored;

(d) to whom that data may then be secondarily disclosed or used under section 300; and

(e) why is the provision of guidance and training to police regarding the applicability and scope of section 287 not sufficient to achieve the aim of this measure.

2.95 The full initial analysis is set out in *Report 6 of 2022*.

Minister's response

2.96 The minister advised:

> Shortly prior to finalisation of the explanatory materials required for introduction of the Bill, a number of non-publication orders were made in relation to the *Inquest into the disappearance of CD*, the findings of which were not yet public at the time. As such, references made to the findings in the Explanatory Memorandum to the Bill were either removed or limited as a precautionary measure.
>
> This was to ensure that the Government did not inadvertently contravene an order through its reliance on any materials provided in confidence before the publication of findings. As the findings are now available online, the Government will issue an updated Explanatory Memorandum and statement of compatibility to address the Committee's concerns.
>
> On 24 November 2022, the Senate referred the Bill to the Environment and Communications Legislation Committee. While described generally in the *Inquest into the disappearance of CD* and the response provided, the Government appreciates the position of law enforcement agencies that outlining specific details about the operational methodology of how missing persons investigations are conducted would expose vulnerable people to unjustifiable risk. My Department considers that this information may be of significant value to the Senate Committee in its appraisal and scrutiny of the Bill, and would be happy to facilitate a discussion with relevant agencies if it is of interest to the Committee.
>
> …
>
> **(a) What is the process by which section 287 is invoked (for example, is it only ever police contacting carriage service providers in practice?), and is a warrant or other formal application a part of the process?**

In practice, the provision generally only applies when a carrier or service provider is contacted by the police.[12]

For the proposed exception in section 287 of the Act to apply, the carrier or carriage service provider must believe on reasonable grounds that the disclosure is reasonably necessary to prevent or lessen a serious threat to the life or health of a person. The Bill will also introduce the safeguard that the carrier or carriage service provider must be satisfied that it would be unreasonable or impracticable to obtain the consent of the person to which the information disclosed relates to. The OAIC's Australian Privacy Principle Guidelines (C.5) on the equivalent use/disclosure principle in the *Privacy Act 1988* provides helpful interpretative guidance about the scope and appropriate meaning of these terms in relation to the circumstances where a use or disclosure is likely to be permitted.

It is the intention of the proposed measure that regulated entities would be largely reliant on the representations made by law enforcement or emergency service organisations to determine whether a threat was 'serious'. This approach is consistent with the existing operational approach of law enforcement agencies, and recognises that law enforcement or emergency service organisations have access to information, systems and resources that telecommunications companies do not.

It is important to note that the amendments to the exception in section 287:

- do not compel the disclosure of information - even in cases where a request from police clearly satisfies the threshold for the exception to apply, disclosure remains at the discretion of the carrier;
- do not provide access to the contents or substance of a communication, or any other information which would ordinarily require a warrant;
- do not allow for information received through the exception to be used for another purpose – the amendments to section 300 of the Act require that any secondary disclosure or use of information by police or emergency service organisations must relate back to the purpose of

12 The Committee could well ask why the provision is not specifically limited to disclosure to law enforcement agencies. However, doing so would be unnecessarily limiting given the range of circumstances that may involve a serious threat to a person's life or health. For example, the provisions were given consideration in the 2009 Black Saturday Bushfires. In that instance disclosure of location information was of assistance to Emergency Service Organisations to issue warnings to save lives. The current drafting of the Act, which the Bill does not modify, recognises that there are an unlimited number of unpredictable circumstances in which an emergency may manifest itself, and which a disclosure may be necessary to save what is most important – human life.

> the original request. Failure to do so is an offence punishable on conviction by 2 years imprisonment.

Rather, the exception provides that a carrier or carriage service provider does not commit a criminal offence for disclosing information about the 'affairs or personal particulars' of a person where it has a reasonable belief that doing so is reasonably necessary for preventing or lessening a threat to the person's life or health.

In relation to missing persons, a formal request from law enforcement agencies to providers is required, but internal procedural requirements also apply for law enforcement to help establish that the thresholds for reasonable belief and reasonable necessity in the exception are met for section 300 of the Act.

This includes mandatory risk assessments, exhaustion of less intrusive methods, and internal authorisation requirements prior to initiating the process for a request. Broadly speaking, this also includes adherence to the Australia New Zealand Policing Advisory Agency *Missing Persons Policy (2020)* and *Guiding Principles*. In both the *Inquest into the death of Thomas Hunt*, and the *Inquest into the disappearance of CD*, a formal request to the provider was never made because NSW Police were not able to satisfy themselves that the threshold could be met by the circumstances.

The Government recognises the particular sensitivity that may attach to the personal information of individuals who have been reported missing. Such individuals may have exercised their free choice to disassociate themselves from friends and family for legitimate reasons, including removing themselves from harmful environments. Accordingly, a claim made by a member of the general public, without support or confirmation from emergency service organisations or law enforcement agencies, would not meet the threshold for the exception to apply. This is made plain in the explanatory memorandum to the Bill. However, the Government will clarify the process through which requests under the section 287 exception are invoked through amendments to the Bill's explanatory materials.

(b) What specific kinds of information may be used or disclosed as a result of the offence provisions not applying. In particular, would it allow for the content of a person's text messages or voicemail or their call log to be made available, or only the GPS phone triangulation;

Section 287 of the Act reads:

> Division 2 does not prohibit a disclosure or use by a person (the first person) of information or a document if:
>
> (a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person.

The exception in section 287 of the Act, and the proposed amendment, does not allow for the content or substance of a communication to be made available in any circumstance. The proposed measure in the Bill will not change or increase the type of information which can be requested and disclosed through the operation of the provision.

The exception only applies to information relating to the 'affairs or personal particulars of a person', a meaning which includes location information as clarified by section 275A of the Act. Carriers do not typically have access to GPS information, and triangulations do not use GPS technology. Instead, a triangulation provides an approximate area of where a handset might be located, based on the location of one or more nearby cell towers. While there can be an enormous variance in the accuracy of this information, triangulations remain a useful tool in missing persons investigations, assisting in locating high-risk missing persons in about 20% of occasions in NSW.

As set out in paragraph 177 of the *Inquest into the Disappearance of CD*, if deemed necessary and proportionate following the initial risk assessment of relevant factors in a missing persons case, consideration may also be given to the use of Live CAD – which provides the time and date of activation of a mobile phone to the network, whether those activations consist of incoming or outgoing calls, and cell tower location.

(c) How such data is managed on receipt, and whether, how, and for how long such data is then stored;

In consultation with law enforcement agencies, the Department understands that the management of such data is received and managed according to well-established protocols, and also subject to a range of safeguards of which only one is the Act (which, for example, prohibits disclosure except in specified circumstances, and for which the penalty is two years imprisonment). These procedures and protocols are not public, to avoid disclosure of operational police practices. The Department can assist to arrange private briefing with law enforcement agencies with the Committee if that would be of assistance. These protocols and practices are also subject to a range of oversight mechanisms, including at the federal level by a number of oversight bodies, including the National Anti-Corruption Commission.

(d) To whom that data may then be secondarily disclosed or used under section 300;

In practice, to law enforcement or Emergency Service Organisations, to the extent that secondary disclosure is necessary (see the discussion above in relation to section 286). The secondary disclosure exception in section 300

of the Act can only be relied upon where doing so was for the purposes of preventing a serious threat, or the first person (i.e. the carrier or carriage service provider) believes on reasonable grounds that the disclosure is reasonably necessary to prevent or lessen a serious threat to life or health.

For example, if a carrier were to rely upon section 287 to disclose triangulation information to the NSW police about a missing person, and the triangulation data showed that the missing person was located in Queensland, the NSW police would be able to rely on section 300 to disclose that triangulation data to Queensland police if the NSW police formed the reasonable belief that doing so would save the person's life.

The Bill introduces a new safeguard into section 300 that it must be impracticable or unreasonable to obtain the consent of the person the disclosure relates to. In doing so, the proposed measures in the Bill ensure that any secondary use or disclosure of information received under these exceptions must be for the authorised purpose, contravention of which is an offence punishable on conviction by 2 years imprisonment.

(e) Why is the provision of guidance and training to police regarding the applicability and scope of section 287 not sufficient to achieve the aim of this measure?

Because even with additional guidance or training, the 'imminent' threat threshold adds nothing to the safeguards in the Act, and the delay making out 'imminence' has contributed to the deaths of at least two people. As the Australian Law Reform Commission pointed out more than 10 years ago, any consideration of a serious threat, will give consideration to imminence if that is of relevance to the matter at hand.[13]

In the *Inquest into the Disappearance of CD*, paragraphs 107-137 of Magistrate Kennedy's findings provide further justification about the ongoing challenges experienced with the interpretation of the provision, and the need for legislative reform. Moreover, the Department consulted the Interception Consultative Committee (ICC) several times in relation to these guidelines, and sought their feedback through several revisions. The ICC is a longstanding government consultative committee led by the Attorney-General's Department (AGD), which includes both police agencies and industry representatives. While the clarification provided by the material was welcomed, it became clear that the 'imminence' qualifier in section 287 of the Act presents a legislative barrier in missing persons investigations that is difficult to overcome through guidance or training alone. In the Inquest into the Disappearance of CD, Chief Inspector Charlesworth of the NSW Police, who refused the request to triangulate CD's mobile phone because there was insufficient evidence the threat was

13 See: For Your Information: Australian Privacy Law and Practice (ALRC Report 108) | ALRC

imminent, confirmed he would make the same decision today with the benefit of hindsight due to the lack of imminence.[14]

Concluding comments

International human rights legal advice

Right to privacy

2.97 In relation to when a carrier may disclose or use information relating to the affairs or personal particulars of another person, the minister advised that in practice, the provision generally only applies when a carrier or service provider is contacted by the police (although it could also be relied on by other emergency services in cases such as bushfires). The minister advised that in relation to missing persons, a formal request from law enforcement agencies to providers is required. The minister stated that internal procedural requirements also apply for law enforcement to help establish that the thresholds for reasonable belief and reasonable necessity in the exception are met for section 300, as well as mandatory risk assessments, exhaustion of less intrusive methods, and internal authorisation requirements prior to initiating the process for a request. The minister also stated that this broadly also requires adherence to existing policies regarding missing persons. As such, it would appear that while a warrant is not required under section 287, a formal application may be required, and additional requirements must be met in the case of a missing person (although noting that such processes are not publicly available). It is less clear what processes would apply where section 287 was sought to be invoked in relation to other potential threats to life and health (for example, in the case of bushfires or other natural disaster). In this regard, it is noted that the minister has advised that there are 'an unlimited number of unpredictable circumstances in which an emergency may manifest itself' where a disclosure may be necessary to save life. This does raise some questions about the processes required to regulate the exercise of this power in circumstances other than that described in relation to missing persons.

2.98 In this regard, it is noted that the minister stated that section 287 does not compel a provider to disclose information to emergency services: 'even in cases where a request from police clearly satisfies the threshold for the exception to apply, disclosure remains at the discretion of the carrier'. However, it is not clear that a provider would reasonably be in a position to dispute an emergency service operator's assertion that a person's life or health is in danger, and so decline to provide the information (or to otherwise simply decline to provide the information). Indeed, as the minister has advised it is 'the intention of the proposed measure that regulated entities would be largely reliant on the representations made by law enforcement or emergency service organisations to determine whether a threat was

14 See: *Inquest into the Disappearance of CD* – NSW Coroner's Court *at* 115.

"serious"'. As such, the absence of a legal power of compulsion would appear to have limited safeguard value. For this reason, the processes regulating the exercise of this power by law enforcement and other emergency services are important considerations.

2.99 As to the types of information that may be disclosed, the minister advised that section 287 does not allow for the content or substance of a communication to be made available in any circumstance. The minister stated that the provision only applies to information relating to the 'affairs or personal particulars of a person', which includes location information (pursuant to section 275A).[15] The minister advised that this provides only approximate information about where a handset may be located, not a precise location. The minister further advised that, if deemed necessary and proportionate following the initial risk assessment of relevant factors in a missing persons case, consideration may also be given to the use of 'Live CAD' – which provides the time and date of activation of a mobile phone to the network, whether those activations consist of incoming or outgoing calls, and cell tower location.[16] The term 'affairs or personal particulars' is not defined in the Telecommunications Act, and so it would appear that section 287 is capable of permitting the disclosure of a broader range of information than merely location information.[17] However, the fact that the content or substance of a communication cannot be disclosed in any circumstances substantially assists with the proportionality of the measure.

2.100 As to how such data is managed on receipt, and whether, how, and for how long such data is then stored, the minister advised that this occurs according to 'well-established protocols', and subject to a range of safeguards, which are themselves subject to a range of oversight mechanisms. The minister stated that these procedures and protocols are not public, to avoid disclosure of operational police practices. Depending on how robust such protocols and safeguards are, their existence would appear capable of serving as important safeguards in the handling of data received pursuant to section 287, which also assists with the proportionality of the measure.

15 The term 'affairs or personal particulars' is not defined in the Telecommunications Act, but section 275A does state that location information is taken to be 'information that relates to the affairs of a customer'.

16 For further information, see e.g. Department of Home Affairs, *Advanced Mobile Location*, 13 September 2021.

17 The Australian Law Reform Commission (ALRC) has previously described 'personal particulars' as a potentially broad category of information which would cover personal information. See, ALRC, *Report 108, For Your Information: Australian Privacy Law and Practice* (May 2008) at [71.20].

2.101 The minister further advised that, in practice, data obtained under section 287 may only be secondarily disclosed or used under section 300, to law enforcement or Emergency Service Organisations, and only to the extent that secondary disclosure is necessary. In this regard, the minister noted that section 300 may only be relied on where doing so is for the purposes of preventing a serious threat, or where the first person (i.e. the carrier or carriage service provider) believes on reasonable grounds that the disclosure is reasonably necessary to prevent or lessen a serious threat to life or health. The minister also noted the proposed introduction of a new requirement that it must be impracticable or unreasonable to obtain the consent of the person to whom the disclosure relates, and that any secondary use or disclosure of information received under these exceptions must be for the authorised purpose, contravention of which is an offence. It would appear, therefore, that the secondary disclosure provision in section 300 is circumscribed such that it may only be relied on in narrow circumstances.

2.102 Further information was also sought as to why the provision of guidance and training to police regarding the applicability and scope of section 287 (a recommendation made by a NSW coroner in 2020) is not sufficient to achieve the aim of this measure. The minister advised that the report into a more recent coronial inquiry—*Inquest into the disappearance of CD* (September 2022)—is now public,[18] and includes recommendations relevant to this matter. The coroner's report outlines the narrow interpretation that had been given to section 287 in this case, including as a result of a narrow interpretation being applied to the 'imminent' qualifier. As to why the provision of guidance and training to police regarding the applicability and scope of section 287 would not be sufficient to achieve the aim of this measure, the minister stated that 'even with additional guidance or training, the 'imminent' threat threshold adds nothing to the safeguards in the Act, and the delay making out 'imminence' has contributed to the deaths of at least two people'. As such, the provision of guidance and training to police as to the scope of section 287 (as currently drafted) is unlikely to be an effective less rights-restrictive alternative.

2.103 Having regard to the detailed information provided by the minister, particularly in relation to the type of personal information that may be obtained under section 287; the circumstances in which the provision may be relied on (typically by police); and the rationale as to why the existing provision is unduly restrictive, on balance this measure would appear likely to constitute a proportionate limit on the right to privacy. However, it is noted many of the safeguards provided above are non-legislative in nature and some safeguards depend on robust internal police processes. In particular, the term 'affairs or personal particulars' is not defined in the Telecommunications Act. Further, while it

18 See, Coroners Court of New South Wales, *Inquest into the disappearance of CD*, 16 September 2022.

appears there is existing guidance the police must follow to use this provision in the context of missing persons, it is less clear if such guidance exists to regulate the exercise of this power in circumstances other than that described in relation to missing persons (for example, by other emergency services personnel in the context of a natural emergency).

Committee view

2.104 The committee thanks the minister for her comprehensive response in relation to this measure, and advice that the findings of a recent coronial inquest to which this measure relates are now publicly available. The committee notes the importance of removing the existing qualifier in section 287 that a threat to the life or health of a person be 'imminent' before a carrier discloses telecommunications data to police and other emergency services personnel. In particular, the committee notes the minister's advice that the delay in making out 'imminence' has contributed to the deaths of at least two people.

2.105 The committee also notes that disclosing personal telecommunications data limits the right to privacy, particularly in circumstances where a person may voluntarily have gone missing and may not wish to be contacted. The committee notes that the right to privacy may be limited where it is reasonable and necessary to do so. In this instance, based on the comprehensive additional information provided by the minister, the committee considers there are, on the whole, sufficient safeguards built into the existing processes to ensure that the limit on the right to privacy is likely to be proportionate. Of particular importance is the minister's advice that this provision would not allow access to the substance of content of communication in any circumstances and there are robust processes in place before the information can be sought.

2.106 The committee considers that the minister's advice sets out the processes the police must follow before invoking this provision in relation to missing persons, and such processes help with the proportionality of the measure. However, the minister's advice did not provide detail of any existing guidance as to the processes followed in cases not involving missing persons. Further, the committee considers there is some risk that the type of information that might be disclosed using these powers is overly broad, noting that disclosure may relate to the ‘affairs or personal particulars of a person’ – a term which is not defined in the legislation.

Suggested action

2.107 If it does not already exist, all emergency service providers who may seek to invoke the powers in section 287 (for example, in the context of natural emergencies) should consider making publicly available guidance as to the process to be followed before requests are made under section 287 to access personal information held by carriers.

2.108 The proportionality of this measure may be assisted were the bill to be amended to define what is captured by the term 'the affairs or personal particulars' of a person, to reflect the limited type of information or documents that the minister advised may be disclosed under the powers in section 287, noting that any such definition should not restrict or frustrate the important intention of this provision.

2.109 The committee welcomes the minister's advice that the explanatory materials accompanying the bill will be updated to include the information provided to the committee by the minister.

Immunity from civil liability

2.110 The bill seeks to amend subsection 313(5)(a) of the Telecommunications Act relating to civil immunities for carriers, carriage service providers and carriage service intermediaries.[19] This amendment would provide that a carrier or carriage service provider or intermediary is not liable to an action or other proceeding for damages for or in relation to an act done (or omitted to be done) in good faith when providing help as is reasonably necessary for specific purposes in connection with preparing for, responding to, or recovering from an emergency.[20]

Summary of initial assessment

Preliminary international human rights legal advice

Right to an effective remedy

2.111 By extending immunity of these bodies from civil liability to include an act done or omitted in good faith when providing help in connection with an emergency, this measure engages the right to an effective remedy. This is because, if such an act done or omitted by a carrier or carriage service provider/intermediary resulted in a violation of a person's human rights (such as the right to privacy), they would be unable to seek a civil remedy for that violation from the various carriers.

2.112 The right to an effective remedy requires the availability of a remedy which is effective with respect to any violation of rights and freedoms recognised by the

19 Item 10.

20 That is, duties established under subsections 313(4A) or (4B)).

covenant.[21] It includes the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the state. While limitations may be placed in particular circumstances on the nature of the remedy provided (judicial or otherwise), States parties must comply with the fundamental obligation to provide a remedy that is effective.[22]

2.113 The statement of compatibility fails to acknowledge the engagement of this right. As such, no information is provided as to whether and how this proposed amendment is consistent with the right.

Committee's initial view

2.114 The committee noted that extending the immunity of carriers and carriage service providers (such as mobile service providers) from civil liability engages the right to an effective remedy. The committee noted that the statement of compatibility does not identify the engagement of this right, and therefore sought the minister's advice as to:

(a) whether the measure is consistent with the right to an effective remedy; and

(b) what alternative remedies are available to persons where performance of a duty under subsections 313(4A) and (4B) results in a violation of their human rights.

2.115 The full initial analysis is set out in *Report 6 of 2022*.

Minister's response[23]

2.116 The minister advised:

> Section 313(5) of the Act provides that a carrier or carriage service provider is not liable to an action or other proceeding for damages if an act is done or omitted in good faith under subsections 313 (1), (1A), (2), (2A), (3) or (4) of the Act. However, it does not include subsections 313(4A) and

21 International Covenant on Civil and Political Rights, article 2(3). See, *Kazantzis v Cyprus,* UN Human Rights Committee Communication No. 972/01 (2003) and *Faure v Australia,* UN Human Rights Committee Communication No. 1036/01 (2005). States parties must not only provide remedies for violations of the ICCPR but must also provide forums in which a person can pursue arguable if unsuccessful claims of violations of the ICCPR. Per *C v Australia*, UN Human Rights Committee Communication No. 900/99 (2002), remedies sufficient for the purposes of article 5(2)(b) of the ICCPR must have a binding obligatory effect.

22 See UN Human Rights Committee, *General Comment 29: States of Emergency (Article 4)* (2001) [14].

23 The minister's response to the committee's inquiries was received on 9 December 2022. This is an extract of the response. The response is available in full on the committee's website.

(4B). The amendment in the Bill is consistent with similar provisions relating to safeguarding national security and public revenue in the Act, and corrects a [sic] error in the National Emergency Declaration Bill 2020, introduced by the former Government.

Under the National Emergency Declaration (Consequential Amendments) Act 2020 (NED(CA) Act), subsections 313(4A) and (4B) were inserted into the Act. These subsections introduce a duty on telecommunications providers to provide reasonably necessary help during certain emergencies.

It was intended that these entities would not be liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in fulfilment of that duty. The policy intention was set out in the Explanatory Memorandum to the National Emergency Declaration (Consequential Amendments) Bill 2020 that immunities would extend to the duties under subsections 313(4A) and (4B). Due to an error in drafting, the measures were not included in the Bill, and unfortunately section 313(5) was not amended to give effect to the then Parliament's intention.

(a) whether the measure is consistent with the right to an effective remedy;

The Government believes that these measures are consistent with the right to an effective remedy, as laid out in Article 2(3)(a) of the International Covenant on Civil and Political Rights (ICCPR).

By extending the existing civil immunities to a carrier or carriage service provider when fulfilling a duty under subsections 313(4A) and (4B) to give officers and authorities of the Commonwealth and of States and Territories such help as is reasonably necessary in disaster and emergency circumstances, including national emergencies, the Bill engages the right to an effective remedy for any unlawful or arbitrary violation to the rights of individuals infringed in the process of providing that help. The proposed extension of the existing civil immunity serves the legitimate objective of ensuring that an officer, employee or agent acting on behalf of a carrier or carriage service provider are able to provide the reasonably necessary help before, during and after disasters and national emergencies, fulfilling their statutory duty in good faith and in the national interest.

The immunities are rationally connected to that important objective by managing the risk that carriers or carriage service providers would limit their conduct and in turn, the level of assistance given to the requesting government body to minimise any real or perceived risk of incurring personal civil liability. The immunity is proportionate to achieving this important objective, it is not arbitrary, unfair or based on irrational considerations and is limited to circumstances where a telecommunications company is assisting in good faith in specified situations (as noted above) and is only related to actions or other proceedings for damages (e.g. a cause of action in tort or negligence).

(b) what alternative remedies are available to persons where performance of a duty under subsections 313(4A) and (4B) results in a violation of their human rights;

While the Government believes that the Bill does engage the right to an effective remedy under article 2(3) of the ICCPR, to the extent that it does limit that right, the limitation is reasonable, necessary and proportionate to the objective. Alternative remedies are available to persons where performance of the duty results in a violation of their human rights.

In cases where the performance of the duty was done in good faith, an affected person could still seek an effective remedy for loss or damage suffered in the purported exercise of the assistance against the relevant Commonwealth, State, or Territory body or government official initiating the request for assistance.

In relation to the right of privacy that the Committee has queried, in giving (requested) help in accordance with subsections 313(4A) and (4B), carriers and carriage service providers must still comply with all applicable laws, including the *Privacy Act 1988* (Cth) and the Act itself. For example, Part 13 sets out strict rules for carriers, carriage service providers and others in their use and disclosure of personal information. A request for help in accordance with subsections 313(4A) and (4B) that included the provision of information would in and of itself not provide the legal basis for a carrier to disclose personal information of an individual (an exception to the prohibition in Part 13 would need to be found).

Private citizens may also seek recourse through other avenues where, in giving help, a carrier or carriage service provider has allegedly interfered unlawfully with an individual's right to privacy. For example, a complaint could be made to the Australian Communications and Media Authority (ACMA) if there was a concern that a carrier or carriage service provider had breached Part 13 of the Act or concerns about how the duties under subsections 313(4A) and (4B) were carried out. The ACMA could take enforcement action against the carrier or provider, including court injunctive relief. Similarly, a complaint could be made by the individual directly to the Privacy Commissioner for investigation (noting that privacy breaches will attract fines etc).

Concluding comments

International human rights legal advice

Right to an effective remedy

2.117 The minister advised that the measure engages, and is consistent with, the right to an effective remedy. The minister noted that this provision only limits liability in respect of actions for damages. The minister advised that alternative remedies would be available to persons where performance of a duty in good faith under subsections 313(4A) and (4B) results in a violation of their human rights. In particular,

the minister advised that a person could bring a claim for loss or damage suffered in the purported exercise of the assistance against the relevant Commonwealth, State, or Territory body or government official initiating the request for assistance. The minister also noted the operation of the *Privacy Act 1988* (Privacy Act), in relation to an unlawful use of information, and the ability of persons to complain to the Australia Communications and Media Authority (ACMA) 'if there was a concern that a carrier or carriage service provider had breached Part 13 of the Act or concerns about how the duties under subsections 313(4A) and (4B) were carried out'. The ACMA could then obtain injunctive relief from a court. Similarly, a person could also complain to the Privacy Commissioner about a suspected privacy breach.

2.118 Having regard to the availability of these alternative remedies in relation to any loss or damage suffered as a result of the performance of a duty (in good faith) under section 313 (resulting in a corresponding violation of human rights, such as the right to privacy), this measure would appear to be consistent with the right to an effective remedy.[24]

Committee view

2.119 The committee considers that, based on the additional information provided by the minister about the availability of other remedies, extending the immunity of carriers and carriage service providers (such as mobile service providers) from civil liability is compatible with the right to an effective remedy. The committee welcomes the minister's advice that the statement of compatibility will be updated to reflect the engagement of this right.

Records relating to authorised disclosures of information or documents

2.120 Items 12–14 of Schedule 1 of the bill seek to amend section 306 of the Telecommunications Act, which establishes the record-keeping requirements where an eligible person or eligible number-database person[25] has disclosed information or

24 In this regard, it is noted that under international human rights law, while limitations may be placed in particular circumstances on the nature of a remedy provided (judicial or otherwise), States must comply with the fundamental obligation to provide a remedy that is effective. This means that, in assessing whether a particular measure is consistent with the right to an effective remedy, the assessment will turn on whether there are sufficient remedies so as to be 'effective' (including considering what alternative remedies are available in spite of the limitation of a particular remedy). The standard limitation test (legitimate objective, rational connection, proportionality), which has been drawn on in the minister's response, is not applicable to this assessment.

25 An 'eligible person' is a carrier; carriage service provider; telecommunications contractor; or employee of such. An 'eligible number-database person' is a number-database operator or contractor, or employee of such. See, Telecommunications Act, ss. 271–272.

a document as authorised by a provision of Division 3 of the Telecommunications Act, or as authorised under specified sections of the *Telecommunication (Interception and Access) Act 1979* (TIA Act).[26]

2.121 The measure would expand the circumstances in which section 306 would require the creation of a record to include where a disclosure has been made pursuant to section 187AA(1) of the TIA Act.[27] Subsection 187AA(1) sets out the kinds of information that a service provider must keep, or cause to be kept. This includes: the name and address of a telecommunications subscriber; the source and destination of their communications (i.e. the device a communication was sent from and where it was sent); the type of communication (e.g. email, voicemail); and the location of the equipment used for the communication (e.g. cell towers or wi-fi hot spots). The bill would provide that, if the information or document that was lawfully disclosed included information of a kind specified in subsection 187AA(1), a record of the disclosure must set out the number of the item[28] and a description of the content of those items to the extent that the content relates to the information or document.

Summary of initial assessment

Preliminary international human rights legal advice

Right to privacy

2.122 Requiring the creation of a record of disclosure under section 306 of the Telecommunications Act engages and limits the right to privacy. This is because the information required to be retained by a service provider under subsection 187AA(1) would include personal information (including the name and address of a service subscriber, and information relating to all of their communications on a device).

2.123 The right to privacy may be subject to permissible limitations which are provided by law and are not arbitrary. In order for limitations not to be arbitrary, the measure must pursue a legitimate objective and be rationally connected to (that is, effective to achieve) and proportionate to achieving that objective.

---

26 Namely, sections 177, 178 or 179, subsection 180(3) or section 180A of the *Telecommunication (Interception and Access) Act 1979*.

27 Specifically, item 15 of the bill would insert a new paragraph 306(5)(g) which would require the creation of a record where the information or document includes information specified in a table that is (a) specified in a determination made by the Minister, by legislative instrument under new subsection 305(5A) (inserted by Item 16); or (b) if there is no determination, the table in subsection 187AA(1) of the *Telecommunications (Interception and Access) Act 1979*.

28 The table in subsection 187AA(1) groups the types of information into six numbered groups. For example, recording the number of the item as 'Item No. 6' would indicate that the information relates to the location of the equipment used in connection with a communication.

Committee's initial view

2.124 The committee noted that expanding the requirement to record where an authorised disclosure of information, including personal information, has occurred engages and may limit the right to privacy and sought the minister's advice as to:

(a) whether the measure is consistent with the right to privacy; and

(b) in particular, what safeguards would operate in respect of information required to be recorded under section 306 (including with respect to requirements for the data's storage, and its destruction after it is no longer required to be retained).

2.125 The full initial analysis is set out in *Report 6 of 2022*.

Minister's response[29]

2.126 The minister advised:

(a) Is the measure consistent with the right to privacy?

(b) What safeguards operate in respect of information required to be recorded under section 306?

The Government does not consider that any aspects of the measure will limit the right to privacy.

Prior to introduction of the Bill, the Office of the Australian Information Commissioner (OAIC) was consulted on an exposure draft of the proposed measures, and requested an additional amendment to include a description of the type of content disclosed. A revision to Clause 13 of the Bill was made to include a requirement to this effect. This measure introduces a requirement to keep a record of the type of information which was disclosed by reference to the table in subsection 187AA(1) of the *Telecommunications (Interception and Access) Act 1979* - e.g. 'subscriber address'; 'billing information; 'call charge record from x date' - to assist in the OAIC's assessment of proportionality.

It does not, however, require providers to record the actual information disclosed, or otherwise retain any personally identifiable information in the record of disclosure. This issue was specifically addressed in consultation with major carriers and the Communications Alliance, and a revision to the explanatory materials of the Bill will be tabled to clarify the intended operation of the measure and that the disclosure record should not contain personally identifiable information.

29 The minister's response to the committee's inquiries was received on 9 December 2022. This is an extract of the response. The response is available in full on the committee's website.

Telecommunication providers subject to the *Privacy Act 1988* will continue to have obligations requiring that reasonable steps must be taken to protect personal information held under Australian Privacy Principle 11.

Concluding comments

International human rights legal advice

Right to privacy

2.127 The minister stated that this measure does not engage the right to privacy, as the requirement to create a record of the type of information which has been disclosed does not require the creation of a record that itself sets out personal information, for example, a customer's address. Rather it requires only the creation of a record that information of that nature was disclosed. The minister explained that this measure does not require providers to record the actual information disclosed, or otherwise retain any personally identifiable information in the record of disclosure. The minister also noted that telecommunication providers subject to the Privacy Act will continue to have obligations to take reasonable steps to protect personal information.

2.128 Noting that the proposed record keeping requirement set out in items 12–14 of Schedule 1 of the bill will not require the creation of an additional record that itself includes any personal information, it would appear that this measure does not limit the right to privacy.

Committee view

2.129 The committee thanks the minister for this response. The committee notes the minister's advice that this additional record-keeping requirement would not lead to the creation of a new record that includes any personal information. As such, the committee considers that this measure does not limit the right to privacy.

2.130 The committee welcomes the minister's advice that a revision to the explanatory materials of the bill will be tabled to clarify the intended operation of the measure and that the disclosure record should not contain personally identifiable information.

Legislative instruments

Data Availability and Transparency (Consequential Amendments) Transitional Rules 2022 [F2022L01260][1]

Purpose	This legislative instrument makes transitional arrangements for the data sharing scheme established by the *Data Availability and Transparency Act 2022* by prescribing six Australian entities as transitional entities, which are taken to be accredited data service providers for the purposes of the Act for a limited transition period
Portfolio	Finance
Authorising legislation	*Data Availability and Transparency (Consequential Amendment) Act 2022*
Last day to disallow	15 sitting days after tabling (tabled in the Senate and House of Representatives on 25 October 2022). Notice of motion to disallow in the Senate must be given by 9 February 2023
Introduced	House of Representatives, 22 September 2022
Right	Privacy

2.131 The committee requested a response from the minister in relation to the rules in *Report 6 of 2022*.[2]

Facilitating access to Australian Government data

2.132 This legislative instrument prescribes six entities[3] as transitional entities for the purposes of the data sharing scheme established by the *Data Availability and Transparency Act 2022* (the Act). Transitional entities are taken to be accredited data

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Data Availability and Transparency (Consequential Amendments) Transitional Rules 2022, *Report 1 of 2023*; [2023] AUPJCHR 13.

2 Parliamentary Joint Committee on Human Rights, *Report 6 of 2022* (24 November 2022), pp. 68-73.

3 Australian Bureau of Statistics, Australian Institute of Family Studies, Australian Institute of Health and Welfare, Commonwealth Social Services Department (DSS), Queensland Treasury, and Victorian Department of Health, see section 7.

service providers (ADSPs) for the purposes of the Act for a transition period (up to 30 July 2025).[4]

2.133 Under the Act, departments and agencies that control Australian Government data are treated as 'data custodians' and may share the data they control with 'accredited users' under a data sharing agreement. This data may be shared through an ADSP, which acts as an intermediary. An ADSP is a provider that is meant to have 'particular expertise in data sharing and the provision of data services',[5] and may provide: de-identification data services; secure access data services; and complex data integration services.[6] Consequently, this measure has the effect that these six entities may facilitate the sharing of Australian government data during the transitional period.

Summary of initial assessment

International human rights legal advice

Right to privacy

2.134 By authorising the provision of controlled access to Australian government data to the six prescribed entities until 30 July 2025, this measure engages and limits the right to privacy.

2.135 The right to privacy is multi-faceted. It comprises respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information.[7] It prohibits arbitrary and unlawful interferences with an individual's privacy, family, correspondence or home.[8] This includes a requirement that the state does not arbitrarily interfere with a person's private and home life,[9] meaning that any interference with a person's privacy—including one provided for by law—should be in accordance with the

4 Section 7.

5 Explanatory statement, p. 1.

6 *Data Availability and Transparency Act 2022* (Data Availability and Transparency Act), sections 16C–16D. This instrument limits the types of services that some of these transitional entities may provide: DSS must not provide secure access services; Queensland Treasury must not provide secure access services and is limited in providing de-identification services; and the Victorian Department of Health is restricted in terms of any of the three services an ADSP can provide (in that any services must be provided by the Centre for Victorian Data Linkage). See, section 5.

7 International Covenant on Civil and Political Rights, article 17.

8 UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)* (1988) [3]-[4].

9 The UN Human Rights Committee further explains that this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons: *General Comment No. 16: Article 17 (Right to Privacy)* (1988).

provisions, aims and objectives of the International Covenant on Civil and Political Rights, and be reasonable in the particular circumstances.[10] It also includes the right to control the dissemination of information about one's private life, and requires that States Parties take effective measures to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it.[11] It also requires that legislation must specify in detail the precise circumstances in which an interference with privacy will be permitted.[12] The right to privacy may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective, and is a proportionate means of achieving it.

2.136 To the extent that the scheme overall seeks to facilitate controlled access to public sector data for specific purposes, this would appear capable of constituting a legitimate objective. Further, to the extent that the prescription of these six entities as 'intermediaries' for a transitional period will facilitate such controlled data sharing, the measure would appear to be rationally connected to that objective.

2.137 The primary issue is whether this measure constitutes a proportionate means by which to achieve the stated objective, having regard to the extent of the interference with the right to privacy and the question of whether the measure is appropriately circumscribed. It is also necessary to consider the presence of safeguards, the possibility of oversight, the availability of review, and any less rights restrictive alternatives. The extent to which this measure is likely to constitute a proportionate limit on the right to privacy also depends on whether the data-sharing scheme itself constitutes a proportionate limit on the right to privacy.[13]

Committee's initial view

2.138 The committee considered further information was required to assess the compatibility of this measure with this right, and as such sought the minister's advice as to:

10 UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)* (1988) [4].

11 UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)* (1988) [10].

12 UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)* (1988) [8].

13 The committee published its consideration of the bill that gave effect to this scheme—the Data Availability and Transparency Bill 2022—in its scrutiny *Report 2 of 2021* and *Report 4 of 2021*. At that time, the committee retained concerns that this scheme, as drafted, may not be a proportionate means by which to achieve its objectives. However, when that bill was passed by the Parliament, it included 251 amendments which were not considered by this committee.

(a) the type of data, the sharing of which these prescribed entities may facilitate as ADSPs, and whether this could include personal information that may be identifiable; and

(b) whether the prescription of these six entities may have particular implications with respect to the right to privacy as it applies to children (including, whether this measure may have the effect of facilitating the sharing of particular information that relates to children, or whether it may facilitate data-sharing agreements that may have a particular impact on children).

2.139 The committee also wrote to the minister asking departmental officials to provide a briefing to the committee secretariat about how the scheme as a whole operates, whether the amendments to the bill establishing the scheme have addressed the committee's previous concerns, and the interaction of this legislative instrument with the scheme as a whole.

2.10 The full initial analysis is set out in *Report 6 of 2022*.

Minister's response[14]

2.140 The minister advised:

> **(a) the type of data, the sharing of which these prescribed entities may facilitate as ADSPs, and whether this could include personal information that may be identifiable.**
>
> The *Data Availability and Transparency Act 2022* (the Act) establishes a scheme authorising Commonwealth bodies to share public sector data with accredited users in a controlled way. The data may be shared directly with an accredited user, or through an accredited data service provider (ADSP) as an intermediary. The scheme is underpinned by strong safeguards, which include:
>
> - That sharing, collection and use of data must be authorised and the privacy protections in the Act must be complied with by all scheme participants, including minimising the sharing of personal information. Penalties apply where actions are not authorised and participants do not comply with the privacy protections;
> - Requirements for the accreditation of scheme participants who are able to request access to data or be an ADSP, including that these entities have the necessary skills and capability to ensure privacy and protection of data; and
> - Establishment of the National Data Commissioner as a regulator of the scheme along with enforcement mechanisms available to them.

14 The minister's response to the committee's inquiries was received on 19 December 2022. This is an extract of the response. The response is available in full on the committee's website.

The Act defines public sector data to mean data that has been lawfully collected, created or held by or on behalf of a Commonwealth body. This also includes ADSP-enhanced data, which is the copy of the shared public sector data collected by the ADSP and any data that results from the ADSP's use of the public sector data shared with them.

Public sector data is defined broadly and captures data that contains 'personal information' and 'sensitive information', as defined by the *Privacy Act 1988* (Cth) (the Privacy Act), as well as data that does not contain personal information.

For example, public sector data could include data generated within a Commonwealth body in the course of developing policies, administering programs and making decisions, as well as data obtained from outside that body, including from other Commonwealth, State and Territory government bodies or other legal persons - such as third party individuals or companies. This means the public sector data shared through an ADSP could include personal information that may be identifiable.

However, the Act prescribes additional requirements that must be met where a Commonwealth body is proposing to share any data that includes personal information within the meaning of the Privacy Act. These requirements, including the privacy protections set out in Part 2.4 of the Act and those in a data code to be made by the National Data Commissioner, must be met before the sharing will be authorised. For example, the Act prohibits the sharing of biometric data under the scheme unless the individual to whom the biometric data relates expressly consents to the sharing.

The *Data Availability and Transparency Regulations 2022* (the Regulations) also prescribes certain secrecy or non-disclosure provisions to ensure highly sensitive data containing personal information is prohibited from being shared under the scheme. For example, data sharing is barred where it is prohibited by the *National Redress Scheme for Institutional Child Sexual Abuse Act 2018*, the *Child Support (Assessment) Act 1989* and *Child Support (Registration and Collection) Act 1988* and the *Witness Protection Act 1994*. Health information data that is held within the My Health Record system, or the health records of current or former immigration detainees, is also barred from being shared under the scheme.

(b) whether the prescription of these six entities may have particular implications with respect to the right to privacy as it applies to children (including, whether this measure may have the effect of facilitating the sharing of particular information that relates to children, or whether it may facilitate data-sharing agreements that may have a particular impact on children).

The Act establishes entities known as ADSPs, who are expert intermediaries in the data sharing process and who provide specialised data services (such as complex integration, secure access, and de-identification) to support sharing by data custodians with accredited users.

The six entities prescribed by the Rules have the same obligations under the Act during the transitional period as though they were an entity accredited by the National Data Commissioner as an ADSP.

As well as the general privacy protections in the Act[15] that protect the personal information of individuals, including children, the Act also has purpose-specific privacy protections for the sharing of personal information that depend on the data sharing purpose of the project.

The involvement of an ADSP as an expert intermediary in a data sharing project could be a privacy enhancing measure.

If data is to be shared for the purpose of informing government policy and programs, or research and development, doing so may require sharing of data to involve an ADSP. For example, where a data custodian uses an ADSP to prepare data for sharing with the accredited user so the data does not include any personal information (performing a de-identification data service), or where sharing is ADSP-controlled access to data. ADSP-controlled access involves access to data within the controlled settings of the ADSP which enhances the privacy of individuals, including children, where their personal information is to be shared.

Requiring ADSP-controlled access means that, rather than a data custodian sharing data with an accredited user so the accredited user stores the shared data in its systems, the data is stored on the ADSP systems and particular designated individuals with appropriate experience, qualifications or training are provided with access to the ADSP systems to use the shared data. The ADSP is able to put a number of controls in place in this environment to significantly reduce the risks associated with sharing personal information.

The Act also requires that any sharing of data is consistent with the data sharing principles in the Act before sharing takes place:

- The project can reasonably be expected to serve the public interest, and appropriate ethics processes will be observed (project principle);
- Data is only made available to appropriate persons, both at the accredited entity level and individual level (people principle);
- Data is only shared, collected, and used in an appropriately controlled environment (setting principle);
- Appropriate protections are applied to shared data (data principle); and

15 The general privacy protections are minimising the sharing of personal information, prohibition of the reidentification of the data that has been de-identified, prohibitions on the storage or access of personal information outside Australia, and a requirement that express consent is always required to share biometric data (see section 16A of the *Data Availability and Transparency Act 2022*).

- The only output of a project is the final output (as agreed by the parties involved in the project) and such output reasonably necessary or incidental to the creation of the final output. The final output must only contain the data reasonably necessary to achieve the applicable data sharing purpose or purposes (output principle).

Before any sharing of personal information, including that of children, can occur, data custodians, accredited users and ADSPs must all be satisfied they have applied each of the five data sharing principles to the project in such a way that, viewed as a whole, the risks associated with the sharing, collection and use of data as part of the data sharing project are appropriately mitigated.

The data sharing agreement covering the project must then specify, among other things, how the project will be consistent with the data sharing principles and how the parties to the agreement will give effect to the principles. For example, imposing controls on what designated individuals of the accredited user may use data containing personal information of individuals, including children, for. The data sharing agreement must also specify the circumstances where the ADSP is to share ADSP-enhanced data containing personal information with the accredited user, and prohibit the ADSP from providing access to, or releasing, ADSP-enhanced data containing personal information in any other circumstances.

Concluding comments

International human rights legal advice

Right to privacy

2.141 As previously noted, the extent to which this measure is likely to constitute a proportionate limit on the right to privacy depends on whether the data-sharing scheme itself constitutes a proportionate limit on the right to privacy. In addition to the minister's response above, the National Data Commissioner and departmental officials provided the secretariat with a briefing about how the scheme operates, whether the amendments to the bill establishing the scheme addressed the committee's previous concerns, and the interaction of this legislative instrument with the scheme.

2.142 In considering the bill that gave effect to this scheme, the committee queried sufficiency of the safeguards in the bill.[16] The bill was amended considerably prior to its passage, and many of the amendments made directly addressed the committee's

16 See, *Report 2 of 2021*, pp. (24 February 2021), pp. 5-18 and *Report 4 of 2021* (31 March 2021), pp. 26-46.

earlier concerns.[17] Several other amendments also assist in the proportionality of its limitation on the right to privacy. For example, the now *Data Availability and Transparency Act 2022* (the Act) includes several explicit privacy protections regulating the disclosure and use of personal information,[18] and the minister is now required to cause periodic review of the operation of the Act to be undertaken.[19] Further, it is noted that aspects of the Data Availability and Transparency Code 2022, registered on 21 December 2022, also directly address privacy concerns raised previously by the committee.[20]

2.143 These amendments to the Act assist with the proportionality of the scheme as a whole, and accordingly with the proportionality of this instrument. Overall, these privacy protections significantly reduce the risk that prescribing these six entities[21] as transitional entities, and therefore as ADSPs, arbitrarily interferes with the right to privacy. It is noted that no entities are yet accredited as users under the Act and, accordingly, no data has yet been shared under the scheme.[22] This raises the question as to why it is necessary to prescribe these six entities as transitional ADSPs up to 30 June 2025, and not a shorter period subject to a requirement that they seek accreditation. Overall, given the intended breadth of the data sharing scheme, and the myriad types of information that may be shared pursuant to the scheme, its proportionality with respect to the right to privacy will depend considerably on the manner in which it is applied, and the strength of its safeguards in practice.

17 In particular: the definition of 'delivery of government services' in section 15 now clarifies the breadth of this provision including as it relates to services that relate to the provision of a benefit, payment or entitlement; a complaint mechanism for members of the public has been established in section 94; and the functions the National Data Commissioner in section 42 no longer require the office-holder to 'advocate for the acceptance of the benefits of sharing and releasing public sector data', thereby addressing an earlier concern regarding the capacity for the Commissioner to provide genuine independent regulatory oversight of the scheme.

18 Part 2.4.

19 Section 142.

20 In particular, the Data Availability and Transparency Code [F2022L01719] provides further detail as to the meaning of 'public interest' for the purposes of the data sharing principles in section 16 of the Act, and 'unreasonable or impracticable to obtain consent' for the purposes of section 16B.

21 Australian Bureau of Statistics, Australian Institute of Family Studies, Australian Institute of Health and Welfare, Commonwealth Social Services Department (DSS), Queensland Treasury, and Victorian Department of Health, see section 7.

22 Data Availability and Transparency Code [F2022L01719], explanatory memorandum, p. 1. In this regard, the minister has stated that data shared under the scheme may relate to children, hence the reference to the rights of children to privacy in the statement of compatibility.

Committee view

2.144 The committee thanks the minister for this response. The committee thanks the National Data Commissioner and departmental officials for their assistance in providing the committee's secretariat with a useful briefing about the operation of the Data Availability and Transparency Scheme.

2.145 The committee notes that 251 amendments were made to the legislation giving effect to this scheme - the Data Availability and Transparency Bill 2021 - before it passed into law. The committee is pleased to note that many of those amendments were made in response to the committee's recommendations and considers that this assists with the proportionality of the scheme with respect to the right to privacy, and therefore with the proportionality of this legislative instrument made for the purposes of the scheme. Overall, these privacy protections significantly reduce the risk that this instrument, in prescribing six entities as transitional entities, and therefore as ADSPs, arbitrarily interferes with the right to privacy.

2.146 However, the committee considers that, noting the wide breadth of the scheme, and the fact that no data has yet been shared under the scheme, much will depend on how the scheme is applied, and the strength of its safeguards, in practice. The committee notes in particular the new requirement in the Act for the minister to cause periodic reviews of the implementation of the scheme. The committee considers that this will be of great value in ensuring important oversight of the scheme and looks forward to the results of these reviews.

2.147 The committee draws its comments to the attention of the minister and the Parliament.

Mr Josh Burns MP

Chair