Ministerial responses — Report 1 of 2023[1]

1 This can be cited as: Parliamentary Joint Committee on Human Rights, Ministerial responses, *Report 1 of 2023*; [2022] AUPJCHR 14.

SENATOR THE HON MURRAY WATT
MINISTER FOR AGRICULTURE, FISHERIES AND FORESTRY
MINISTER FOR EMERGENCY MANAGEMENT

MS23-000111

Mr Josh Burns MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Chair

I write in response to your correspondence of 25 November 2022 requesting further information in relation to proposed amendments to the *Biosecurity Act 2015* (Act) contained in the Biosecurity Amendment (Strengthening Biosecurity) Bill 2022 (Bill). I wish to apologise for the late reply to your letter and thank the Secretariat for agreeing to an extension for my response.

I note that the Bill passed through the Parliament on 29 November 2022. Nevertheless, I supply the following responses to the committee's request for further information to assist the committee's consideration of the amendments:

Entry requirements

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 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.

Preventative biosecurity measures

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.

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.

Information management framework

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 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, 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.

I have copied the Minister for Health and Aged Care, the Hon Mark Butler MP, into this correspondence as the suggested amendments relate to provisions relevant to the Health portfolio.

I thank the committee for raising these issues for my attention.

Yours sincerely

MURRAY WATT 19 / 01 / 2023

cc: The Hon Mark Butler MP, Minister for Health and Aged Care

Attorney-General

Reference: MS22-0025211

Mr Josh Burns MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

By email: human.rights@aph.gov.au

Dear Mr Burns

Thank you for your email of 25 November 2022 regarding the Parliamentary Joint Committee on Human Rights *Report 6 of 2022* request for information about issues identified in relation to the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill). The Bill passed both houses of Parliament on 28 November 2022.

In relation to the application of the increased penalty under section 13G of the *Privacy Act 1988* (Privacy Act) to persons other than body corporates, the Committee asked for advice on:

- the types of individuals regulated under the Privacy Act, and whether any individuals would be covered by the provision who may not fully understand the regulatory context
- examples of the types of conduct that may constitute a serious or repeated interference with privacy with respect to conduct by individuals, and
- in those instances, why requiring the courts to apply a higher civil standard of proof would not be appropriate.

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.
- 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.

I trust this information is of assistance.

Yours sincerely

THE HON MARK DREYFUS KC MP
8 / 12/2022

OFFICIAL

The Hon Michelle Rowland MP

Minister for Communications

Mr Josh Burns MP
Chair
Parliamentary Joint Committee on Human Rights
By email: human.rights@aph.gov.au

Dear Chair

Thank you to your letter of 25 November 2022 regarding the Parliamentary Joint Committee on Human Rights (Committee) *Report 6 of 2022*, which requests further information to assist its scrutiny of the *Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022* (the Bill).

I appreciate the time the Committee has taken to consider the Bill, and for the opportunity to clarify the operation of the proposed amendments and their engagement with certain rights.

I enclose a response to the request for information made by the Committee in relation to the Bill.

Furthermore, I note the Committee's suggestions to update the Bill's statement of compatibility. The Government will address the recommendations as set out in the report and update the Explanatory Memorandum and statement of compatibility to the Bill accordingly.

Yours sincerely

Michelle Rowland MP

9 / 12 / 2022

Encl. *Response to scrutiny report of the Committee*

Australian Government

Department of Infrastructure,
Transport, Regional Development,
Communications and the Arts

Response to Parliamentary Joint Committee on Human Rights

Telecommunications Legislation Amendment (Information Disclosure, National Interest, and Other Measures) Bill 2022 (the Bill)

In its *Report 6 of 2022,* the Parliamentary Joint Committee on Human Rights (the Committee) considered that further information was required in order to assess compatibility of the Bill with certain human rights, and sought advice in relation to the requested information.

The Bill seeks to improve the functioning of the *Telecommunications Act 1997* (the Act) by clarifying existing provisions, improving their operation and by introducing new safeguards. The most important measure in the Bill improves the ability of police to find missing people – in two recent coronial inquests, it was found that a specific provision of the Act may have contributed to the deaths in question.

The Government does not accept that the Bill reduces, in any way, the right of privacy, and in many areas, the Bill introduces new privacy safeguards into the existing Act. Furthermore, the Bill engages and enhances other rights, such as the right to life as specified in Article 6 of the International Covenant on Civil and Political Rights. Considering drafting improvements and the safeguards introduced, the Bill strikes the right balance to enhance the right of privacy and assist emergency service organisations in finding people and protecting lives.

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.

Attachment A provides a factsheet in relation to the Bill.

GPO Box 594, Canberra ACT 2601, Australia
• telephone • websites infrastructure.gov.au | arts.gov.au

Increased Access to the Integrated Public Number Database (IPND)

Committee view

The Committee requires further information in order to assess the compatibility of this measure with the right to privacy, and has requested advice from the Minister 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).

Minister's response

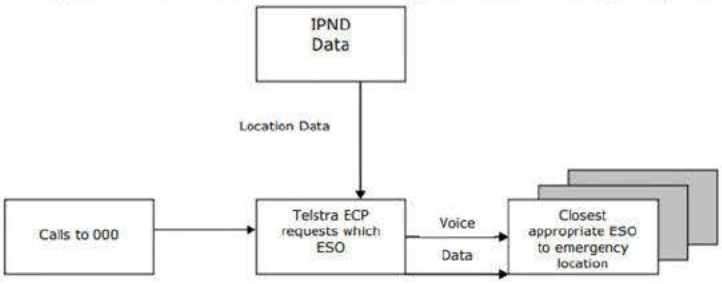
(a) To whom may information obtained under this measure be disclosed, with examples of disclosure?

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.

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[1].

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.

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



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,[2] 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 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.

[1] 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.

[2] See: *Telecommunications (Carrier Licence Conditions - Telstra Corporation Limited) Declaration 2019*

(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.

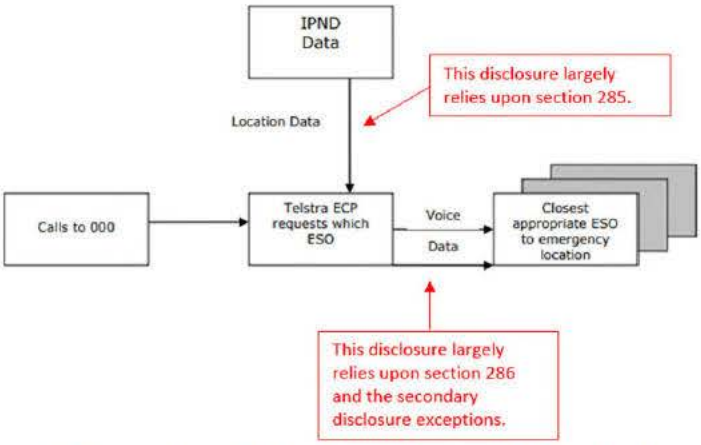


Figure 2: An overview of which provisions apply to which disclosures

(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.[3] Obligations on IPND access seekers are specified in an enforceable industry code[4] and in the data access agreements with Telstra.[5] These technical implementations limit the ability for disclosures to occur for purposes or to entities separate to those mentioned above.

[3] 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.
[4] See: Integrated Public Number Database C555:2020 *(industry code registered under Part 6 of the Act)*;
[5] 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

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

Committee view

The Committee requires further information in order to assess the compatibility of this measure with the right to privacy, and has requested advice from the Minister 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;
(b) what specific kinds of information may be used or disclosed as a result of the offence provisions not applying. 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 data is managed on receipt, and whether, how, and for how long such data is 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.

Minister's response

(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.[6]

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

[6] 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.

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 <u>any</u> 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; and

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.[7]

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 imminent, confirmed he would make the same decision today with the benefit of hindsight due to the lack of imminence.[8]

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

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

Immunity from civil liability

Committee view

The Committee notes that the statement of compatibility does not identify the engagement of the right to an effective remedy, and has requested advice from the Minister as to:

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

Minister's response

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 (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 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).

Records relating to authorised disclosures of information or documents

Committee view

The Committee requires further information in order to assess the compatibility of this measure with the right to privacy, and has requested advice from the Minister as to:

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

(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).

Minister's response

(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.

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.

The Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022 (The Bill) – Fact sheet

Helping Police Find Missing Persons

On 16 September 2022, NSW Deputy State Coroner, Magistrate Erin Kennedy, released her findings on the *Inquest into the disappearance of CD*:

> *"The need for potential amendment of s 287 (of the Telecommunications Act 1997) and the **'serious and imminent'** threshold test requires urgent consideration."*[1]

In response to the Deputy State Coroner's recommendation to reform the *Telecommunications Act 1997* (Tel Act), the Government has introduced a Bill aimed at saving lives, into the Australian Parliament.

- Telecommunications companies are prohibited from disclosing information about their customers. The penalty for disclosure is 2 years imprisonment.
- There are some limited exceptions. One exception, known as section 287, is where sharing information about a customer is needed to prevent or lessen a serious and imminent threat to a person's life or health.
- This provision is used by police and emergency service organisations to get help from telecommunications companies to find missing people using 'triangulation'.
- Triangulation allows telecommunications carriers to estimate the location of mobile phone based on the cell towers that the phone is connected to.
- Triangulation is not perfect – it can only estimate where a phone is – but it is hard to overestimate how important it is in helping police to save lives.
- In missing people cases, time is of the essence. Delays in getting triangulation data can cost lives. In two recent cases, NSW State coroners have highlighted how difficult it is for telecommunications companies and police to reach a conclusion that a threat to a missing person is 'imminent'.
- In fact, NSW Deputy State Coroner, Magistrate Erin Kennedy in the inquiry of into the disappearance of CD has said that reform to section 287 is urgent.
- The Government has introduced a new bill into the Parliament to solve this problem, to help police save lives.
- The bill removes the requirement that telecommunications companies need to reach the conclusion that a threat is imminent. They still need to believe the threat is serious – as the Australian Law Reform Commission has noted, consideration of whether a threat is 'serious' will include consideration of imminence.
- The Government believes that helping police save lives is of utmost importance, but also wants to improve privacy protections. That is why the bill includes new privacy protection safeguards.
- For example, the bill introduces a requirement that it is 'unreasonable' or 'impracticable' to get the consent of the person involved. The Act also includes strict 'secondary disclosure' prohibitions that have been strengthened in the bill – meaning that police are only allowed to use information from telecommunications companies for the purposes that it has been provided for.
- Taken altogether, the bill strikes the right balance, will contribute to saving lives, and will help police to do their critical jobs in finding missing people.

---

[1] Inquest into the disappearance of CD, paragraph 197

"Legislative amendment is of course a matter solely within the province of Parliament. However, it is consistent with my death prevention role to highlight the urgent need for review given the current construction and operation of s 287 in the context of missing person investigations, as was highlighted by this Inquest and that of the Thomas Hunt Inquest."[2]

The case of CD

On 17 June 2019, CD, a NSW man went missing. On 21 June 2019, a NSW Police Detective contacted the Duty Operations Inspector, requesting triangulation of CD's phone. This request was declined on the basis there was no 'serious or imminent threat to the life or health' of CD within the meaning of the Act.[3].

The Chief Inspector who denied the triangulation has expressed his frustration in the position he was in, as he felt legally obliged to decline the triangulation in this case, and articulated the need for legislative change.[4]

The Detective Chief Inspector (DCI) managing the Missing Persons Registry at NSW Police reviewed the investigation into CD's disappearance and formed the following opinion: "... I also believe a triangulation should have been requested to discover the location of CD's phone". The DCI believes the triangulation tool should be used for all 'high risk' missing persons investigations.[5]

The case of Thomas Hunt

On 22 March 2017, Thomas Hunt went missing. As part of the effort to find Thomas, two NSW police officers raised the possibility of organising the triangulation of Thomas' phone. However, despite concerns of Thomas' mental health, police were not confident that they would be able to make out 'imminent threat' threshold, and a triangulation request was not made.[6]

NSW State Coroner, Magistrate Teresa O'Sullivan commented that "it is therefore of some concern that the bar is set high for applications under s. 287 [the relevant provision of the Act] by the State Coordination Unit".[7]

Why is it important to help police find missing people?

In Australia a missing person is anyone who is reported missing to police, whose whereabouts are unknown, and where there are fears for their safety or welfare.

Unfortunately, missing people in Australia is a serious problem.

An estimated 38,000 people are reported missing to police each year; that is one person every 15 minutes.

A long-term missing person is someone who has been missing for more than three months. There are over 2,500 people listed as a long-term missing person.

The increased occurrence of natural disasters over the last few years during the summer period has the potential to heighten missing persons statistics.

If you have concerns for someone's safety and welfare, and their whereabouts is unknown, you can file a missing person's report at your local police station.

"...the decision whether to triangulate can be a matter of life and death".[8]

---

[2] Inquest into the disappearance of CD, paragraph 136
[3] Inquest into the disappearance of CD, paragraph 48
[4] Inquest into the disappearance of CD, paragraph 123
[5] Inquest into the disappearance of CD, paragraph 95
[6] Inquest into the disappearance of Thomas Hunt, paragraph 62
[7] Inquest into the disappearance of Thomas Hunt, paragraph 67
[8] Inquest into the disappearance of CD, paragraph 127

COMMON QUESTIONS/ASSUMPTIONS ABOUT THE BILL

Q: Does the legislation make it easier for abusers to track down victims of domestic violence?
A: No. The changes will only allow for information to be disclosed by a telecommunications company (telco) where there is a serious threat to life or a person's health and where it is impracticable or unreasonable to obtain the consent of the person in question. A telco would be relying on the advice of law enforcement and/or emergency services organisations, in accordance with existing practices. A claim made by a member of the general public, without support or confirmation from law enforcement agencies, would not meet the threshold for disclosure.

Q: Does the legislation reduce privacy protections?
A: No. The changes improve privacy protections. Whilst the 'imminent' qualifier has been deeply problematic and may very well have contributed to loss of life, the changes to the legislation insert a requirement that disclosure from the telco can only occur where is it is impracticable or unreasonable to obtain the consent of the person in question.

Q: Will police get access to my GPS data when they triangulate my phone data?
A: No. Triangulations by carriers do not use GPS technology. A triangulation uses one or more cell towers to provide an approximate area where the handset may be located. Triangulations assist in locating missing persons in about 20% of high-risk missing persons cases in NSW.

Q: Why does there need to be reasonable belief? Why can't it be reasonable suspicion?
A: The use of 'reasonable belief' is consistent with equivalent provisions set out in the Privacy Act. The lower-threshold of 'reasonable suspicion' would create inconsistencies with the Privacy Act if it was applied to the Telecommunications Act.

The Government's approach is consistent with the Australian Privacy Principle Guidelines, where the 'reasonable suspicion' test is used for things like misconduct or unlawful activity, while the higher-threshold of 'reasonable belief' is to be used for locating a person reported missing.

Senator the Hon Katy Gallagher

Minister for Finance
Minister for Women
Minister for the Public Service
Senator for the Australian Capital Territory

REF: MC22-004628

Mr Josh Burns MP
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6022
Parliament House
CANBERRA ACT 2600

Dear Mr Josh Burns

Thank you for your correspondence of 25 November 2022 on behalf of the Parliamentary Joint Committee on Human Rights concerning the *Data Availability and Transparency (Consequential Amendments) Transitional Rules 2022* [F2022L01260].

In its Report 6 of 2022, the Committee requested further information about human rights issues in relation to this legislative instrument. Responses to the Committee's questions are attached for the Committee's consideration.

The Committee also requested that departmental officials provide a briefing to the Committee Secretariat about how the data sharing scheme as a whole 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 as a whole. Officials from the Office of the National Data Commissioner are in contact with the Secretariat to organise a briefing on the data sharing scheme in January 2023.

I appreciate the extension until 19 December 2022 to provide the response.

Yours sincerely

Katy Gallagher

19/12/22

Response to Parliamentary Joint Committee on Human Rights

Report 6 of 2022 – Data Availability and Transparency (Consequential Amendments) Transitional Rules 2022 [F2022L01260]

In its Report 6 of 2022, the Parliamentary Joint Committee on Human Rights (the Committee) sought further information from the Minister in relation to the *Data Availability and Transparency (Consequential Amendments) Transitional Rules 2022* [F2022L01260] (the Rules).

Committee comments made in the Report:

"The Committee considers further information is required to assess the compatibility of this measure with this right, and as such seeks the minister's advice as to:

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)."

Minister's response

(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.

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[1] 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

---

[1] The general privacy protections are minimising the sharing of personal information, prohibition of the re-identification 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*).

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
- 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.