The Hon. David Littleproud MP

Minister for Agriculture and Water Resources
Federal Member for Maranoa

Ref: MC18-035975

27 NOV 2018

Senator Helen Polley
Senate Scrutiny of Bills Committee
SUITE 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator Polley

Thank you for the Scrutiny of Bills Committee's letter dated 15 November 2018 about the Agricultural and Veterinary Chemicals Legislation Amendment (Streamlining Regulation) Bill 2018.

I provide the following to assist with the committee's concerns.

Why it is considered necessary and appropriate to leave all of the content of the proposed accreditation scheme to delegated legislation

The Australian Pesticides and Veterinary Medicines Authority (the APVMA) was established as the independent regulator of agricultural and veterinary (agvet) chemicals up to, and including, the point of supply (e.g. retail sale). In performing this role, the APVMA is required to ensure that chemical products are safe for humans, animals, plants and the environment. The APVMA must also be satisfied with the efficacy of chemical products and that their use would not unduly prejudice Australia's international trade.

In many cases—particularly in respect to new chemicals or uses on pests or crops for which the substance has not previously been authorised—the APVMA forms its satisfaction on the basis of scientific assessments of complex data. The requirements for the APVMA's satisfaction are not prescribed in legislation but are, rather, a matter for the APVMA's professional and scientific judgement.

The measure supports the APVMA's ongoing independence. The proposed scheme would continue, and strengthen, the current practice whereby it is entirely within the APVMA's remit to develop the technical requirements for scientific assessment, which can be readily amended as the science develops. Importantly, the amendments do not authorise any delegation of decision making under the agvet legislation. The APVMA will remain, in all cases, the decision maker.

Before registering a chemical product, the APVMA must reach satisfaction in relation to the safety, efficacy, trade and labelling criteria. The proposed scheme will provide flexibility in how the APVMA may efficiently obtain a robust assessment of applicant's data to assist it to reach this satisfaction (or, alternatively, refuse the application). This may, for example, include specifying the particular types of applications that may be suitable for external assessment. For instance, third-party assessments could involve detailed scientific assessments of complex data for new products, or they could be limited to essentially administrative assessments of applications for products of low regulatory concern with well understood chemistries. Different requirements could also apply in relation to different aspects of assessments, such as toxicology, environmental safety, residues or chemistry. The APVMA is best placed to determine these requirements for any third-party accreditation scheme.

In addition, rather than creating a significant regulatory scheme, the accreditation scheme will be constrained and will, in effect, supplement and formalise existing practices. The APVMA already has a pilot administrative scheme for external assessors, whereby applicants may engage third-party assessors (from a list of assessors currently maintained by the APVMA) to conduct pre-application assessments of efficacy and target crop or target animal safety. By formalising these existing arrangements, the measure in the Bill would provide a more rigorous and transparent framework that would provide a greater basis for public confidence about the assessment of chemicals.

The type of persons who could become accredited assessors would be constrained to those with the particular expertise and knowledge necessary for conducting assessments for the approval of agvet chemicals. As such, the scheme would not have application to the broader Australian public. In addition, as the scheme would be prescribed under the schedule to the *Agricultural and Veterinary Chemicals Code Act 1994* (Agvet Code), regulations could authorise recovery of the APVMA's costs of accrediting assessors.

Adjustments to the scheme may also be necessary from time to time, to adapt to changes in the science and best-practice methodology for assessing agvet chemicals; to respond to lessons learnt from its implementation; or to ensure the integrity of Australia's agvet chemical regulatory framework if issues are identified. Placing detailed content of the proposed accreditation scheme in primary legislation may inhibit the APVMA from making timely adjustments to assessor accreditation and operational requirements. In a worst case, the APVMA might not otherwise be able to rely on the standard of accredited work in deciding its satisfaction that the statutory criteria have been met.

The use of third party accreditation schemes by Commonwealth regulators is not unusual, nor is it unusual for the content of such schemes to be set out in delegated legislation. For example, the Australian Maritime Safety Authority (AMSA), as a national regulator, relies on the recommendations of marine surveyors to determine whether a vessel meets safety standards. The Marine Surveyor Accreditation Scheme is how AMSA ensures that marine surveyors have the appropriate qualifications, capabilities and experience to survey domestic commercial vessels. Details of the accreditation scheme are in delegated legislation—the *Marine Safety (Domestic Commercial Vessel) National Law Regulation 2013*.

The creation of a pool of experienced third-party assessors will not just assist the APVMA, it will also assist industry in preparing applications, particularly emerging or new participants. However, there will be no requirement for industry to engage accredited assessors.

The appropriateness of amending the bill so as to include at least high-level guidance as to the requirements of the proposed accreditation scheme

Item 43 of Schedule 1 in the Bill proposes a new subsection 6G(2), which provides a list of matters that the APVMA may include in the relevant instrument. While not intended to be exhaustive, this subsection provides sufficient guidance as to matters that should be considered in the design of the proposed accreditation scheme.

Proposed new subsection 6G(2) under Item 43, would not be unique in Commonwealth law. For example, section 160 of the *Marine Safety (Domestic Commercial Vessel) National Law Act 2012* provides a regulation making power relating to accreditation and approval (subsection 160(1)) and then provides a list of examples of matters that the regulations may deal with (subsection 160(2)). The *Marine Safety (Domestic Commercial Vessel) National Law Regulation 2013* then provides the requirements of the accreditation and approval scheme.

In addition, for the reasons outlined for the previous question, guidance beyond that proposed in new subsection 6G(2) under Item 43 is not considered appropriate or necessary for the APVMA in developing the requirements for the proposed accreditation scheme.

Whether specific consultation obligations (beyond those in section 17 of the *Legislation Act 2003*) can be included in the legislation (with compliance with such obligations a condition of the validity of the legislative instrument)

The APVMA is already empowered to create legislative instruments related to various matters, including key elements such as determining the efficacy of a chemical product and making standards. The APVMA routinely undertakes consultation when developing legislative instruments, by issuing an exposure draft and calling for public comment. Significant issues raised by respondents are further considered through targeted consultation with the affected parties. The APVMA, and industry, are therefore quite practised in undertaking broad consultation when developing such instruments. Including additional specific consultation requirements for the accredited assessor scheme instrument would misalign with these existing, and well understood, requirements within the APVMA's legislative instrument making framework.

Mandating consultation requirements in the primary legislation may limit the APVMA's ability to respond to urgent situations. Such situations include where the integrity of Australia's agvet chemical regulation framework could be compromised or where the pace of relevant science is outstripping the pace by which consultation can be conducted in accordance with the requirements set out in the primary legislation. As outlined above, it is important to ensure the APVMA's independence as a regulator and support its ability to act swiftly and appropriately to maintain the integrity of Australia's agvet chemical regulatory framework.

I trust this information is of assistance to the committee.

Yours sincerely

DAVID LITTLEPROUD MP

SENATOR THE HON MITCH FIFIELD
MINISTER FOR COMMUNICATIONS AND THE ARTS
MANAGER OF GOVERNMENT BUSINESS IN THE SENATE

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600
scrutiny.sen@aph.gov.au

Dear Senator Polley Helen

Copyright Amendment (Online Infringement) Bill 2018

I refer to the request from the Senate Scrutiny of Bills Committee (the Committee) for an explanation of certain aspects of the Copyright Amendment (Online Infringement) Bill 2018 (the Bill), which seeks to amend the website blocking scheme contained in section 115A of the *Copyright Act 1968* (the Copyright Act).

Specifically, the Committee has sought advice on the operation of item 9 of the Bill, which would introduce new subsection 115A(8B) to the Copyright Act. This new subsection would give the Minister the power to declare, by legislative instrument, that a particular online search engine provider, or an online search engine provider that is a member of a particular class, must not be specified in an application for an injunction under subsection 115A(1), or an application to vary an injunction under subsection 115A(7).

The Committee has sought my advice as to why this new legislative power is necessary, and why the primary legislation does not provide for the determination of what would constitute an online search engine provider.

There are sound reasons for the approach that has been taken in the Bill, which I outline below. The threshold issue relates to the difficulty of defining an online search engine provider in primary legislation, and the risks that would be associated with doing so. The online search engine market is rapidly developing. Even during the time that the website blocking scheme has been operating, since 2015, we've seen significant advancements, particularly as voice search and digital home assistants have emerged in the market. Search functionality is also in-built, to varying degrees, into virtually all websites and apps. I expect the types and range of search engine services will continue to develop rapidly, but I cannot foresee the nature of these developments.

Search engine providers are also not specifically defined in other Australian statutes, beyond the Copyright Act. In addition, the vast majority of international jurisdictions, including the European Union (EU), also do not have such definitions in their legislation. The EU is contemplating whether to define search engine providers in their laws, but it is yet to do so. While the Government has no in-principle opposition to developing a statutory definition in

the long term, it is prudent to monitor international efforts and their outcome before introducing such a definition into Australian law.

For these reasons, the Bill does not seek to define online search engine provider, allowing the Federal Court to make such judgements in respect of online search engine providers within the parameters of the website blocking scheme. However, the Explanatory Memorandum makes clear that the intent of the extension of the website blocking scheme to online search engine providers is not to capture smaller operators or those sites and services for which search functionality is peripheral to their activities. The Explanatory Memorandum states that:

> The intent is that the scheme will enable injunctions to be sought against major internet search operators that index search results on the World Wide Web and are likely conduits to online locations that host infringing material. It is not intended to capture: smaller operators that do not have the same reach; entities that offer internal (intranet) search functions, entities that provide search services to employees, members or clients that are confined to discrete sites (such as educational and cultural institutions, not-for-profit organisations); or entities that provide search functionality that is limited to their own sites or to particular content or material (such as real estate or employment websites or the National Library of Australia's Trove search).

In addition, the Government has included in the Bill a reserve power for the Minister to declare that a person is not an online search engine provider, or that a class or persons are not online search engine providers. As noted in the Explanatory Memorandum:

> The declaratory power in subsection 115A(8B) will provide a safety net, in addition to the built-in safeguards in subsection 115A(5) of the Act (including, for example, the proportionality principle and public interest considerations), to ensure that applications for injunctions do not unfairly target smaller operators that do not have the same reach or entities that provide only internal (intranet) or limited search functions.

I note that the Committee has queried why the Government didn't adopt the approach of a statutory exclusion of certain classes of smaller providers of search engine services. This is for the same reasons as outlined above in relation to the broader statutory definition of online search engine provider. A statutory exclusion would run the risk of failing to accurately intended parties, given the rapid changes underway in the market and the development of products and services that employ search functionality in some form.

The proposed approach of a reserve declaratory power for the Minister provides a more flexible way of dealing with the potential – although small – that an injunction is brought against a party to which these provisions were not intended to apply. The likelihood of this occurring is almost negligible.

Applicants seeking a website blocking injunction under section 115A of the Copyright Act will only do so with respect to a limited number of parties, where the cost and time associated with a Federal Court case are justified relative to the impact of the alleged copyright infringement. In cases to date, applicants have only sought an injunction against a very limited number of major carriage service providers – Telstra, Optus, Vodafone Hutchison Australia, TPG and Vocus. There have been no applications against the hundreds of other smaller carriage service providers, reflecting the fact that it is not in the interests of copyright owners to pursue these smaller providers.

In addition, in determining whether to grant an injunction, the Court may take into account a range of factors set out in subsection 115A(5) that would mitigate the chances of an injunction being granted against smaller search engine providers, or providers of services that include search functionality as a peripheral activity. For example, the Court may consider

whether not providing search results that refer users to the online location is a proportionate response in the circumstances, or in the public interest. These factors will operate to discourage copyright owners from seeking injunctions against small operators or entities that are not intended to be online search engine providers.

In sum, the instrument-making power in proposed subsection 115A(8B) is intended to provide a 'safety-net'. Although it is highly unlikely that this power would ever be exercised, any declaration made under the new subsection 115A(8B) would be a legislative instrument and therefore subject to Parliamentary scrutiny and disallowance.

Thank you to the Committee for requesting this advice. I trust this information will be of assistance.

MITCH FIFIELD

22/11/18

The Hon Dan Tehan MP
Minister for Education

Parliament House
CANBERRA ACT 2600

Telephone: 02 6277 7350

Our Ref: MC18-005164

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

16 NOV 2018

Dear Senator Helen,

Thank you for the email from your Committee Secretary of 18 October 2018 requesting further information on the Higher Education Support (Charges) Bill 2018 and Higher Education Support Amendment (Cost Recovery) Bill 2018 (the Bills).

I appreciate the Committee's consideration of the Bills and I have responded to the issues raised in the Committee's Scrutiny of Bills Digest 12 of 2018 below.

Higher Education Support (Charges) Bill 2018

1.21 The committee requests the minister's advice as to why there are no limits on the charge specified in primary legislation and whether guidance in relation to the method of calculation of a maximum charge can be specifically included in the bill.

Further explanation of the annual charge

The purpose of the Higher Education Support (Charges) Bill 2018 (Charges Bill) is to provide for the application of an annual charge on higher education providers, which is separate from education legislation, and for the annual charge amount to be prescribed in regulations. This is in line with the Australian Government's cost recovery policy that where appropriate, non-government recipients of specific government activities should be charged some or all of the costs of those activities.

As outlined in the Explanatory Memorandum for the Charges Bill, the purpose of setting the amount of the charge for a year via a legislative instrument is to ensure that the charge can be reviewed and updated annually, which will assist providers by giving them certainty on the annual charge amounts for each calendar year.

In addition, there is existing legislation (*VET Student Loans (Charges) Act 2016*) for similar annual charge on VET Student Loans approved course providers that does not provide a limit on the charge, and the amounts for the charge are set out in legislative instrument. This sets a precedent, which was used to guide the development of the Charges Bill.

I consider the current provision (subclause 7(2) of the Charges Bill) providing that before the regulations are made, the Minister must be satisfied that the effect of the regulations will recover no more than the Commonwealth's likely costs for the administration of HELP to be sufficient. The charges calculation methodology and appropriate charge amounts must also comply with and meet the requirements of the Australian Government Cost Recovery Guidelines prior to the creation of the regulations. The detail on the annual charge in the regulations will also be subject to Parliamentary scrutiny as it will be a disallowable instrument, thereby subject to disallowance for 15 sitting days after tabling in both houses of parliament.

My department has also released a 'HELP charging measures cost recovery implementation statement' for consultation with the higher education sector, which will further facilitate transparency and accountability.

Higher Education Support Amendment (Cost Recovery) Bill 2018

1.26 The committee seeks the minister's advice as to why it is considered necessary and appropriate to provide that the rate of a penalty for late payment and the right of review of decisions made in relation to the collection or recovery of higher education provider charges may be set out in delegated legislation.

1.27 The committee also seeks the minister's advice as to why, if it is considered appropriate to leave such matters to delegated legislation, the bill does not require that the Guidelines make review rights available.

Specifying certain matters in delegated legislation

The purpose of the Higher Education Support Amendment (Cost Recovery) Bill 2018 (Cost Recovery Bill) is to amend the *Higher Education Support Act 2003* (HESA) to put in place an application fee on applicants seeking approval as higher education providers under HESA, and to reflect the introduction of an annual charge on higher education providers under the Higher Education Support (Charges) Bill 2018.

Subordinate legislation provides greater flexibility in addressing changes to matters under proposed subsection 19-66(2) of the Cost Recovery Bill each year, instead of pursuing amendments through primary legislation. In addition, administrative issues related to the higher education provider charge and application fee (i.e. the setting of the rate of a penalty for late payment, and right of review of decisions made in relation to the collection and recovery of the annual charge and application fee) are best addressed outside the Cost Recovery Bill. This facilitates a more timely and efficient response to administrative changes for the cost recovery charges.

In addition, there is existing subordinate legislation (*VET Student Loans Rules 2016*) for the collection and recovery of the approved VET Student Loans course provider charge that provides for late payment penalty. This sets a precedent, which was used to guide the development of the Cost Recovery Bill.

Therefore, I consider delegated legislation the appropriate mechanism for setting out matters referred to in the proposed subsection 19-66(2) of the Cost Recovery Bill.

I also note the committee's comments that while the proposed subsection 19-66(2) in the Cost Recovery Bill would allow the *Higher Education Provider Guidelines 2012* (the Guidelines) to include options for review of such decisions, the Bill does not require the Guidelines to include review rights. In response, although the Bill does not require the Guidelines to include review rights, I will undertake to ensure that review rights are included in the Guidelines.

Thank you for bringing these matters to my attention. I trust that my response assists the committee in its understanding of the Bills.

DAN TEHAN

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

Ref No: MS18-009588

Senator Helen Polley
Chair
Senate Standing Committee for the
Scrutiny of Bills
Parliament House
CANBERRA ACT 2600

Dear Senator

Thank you for your correspondence of 19 October 2018 requesting further information on the Telecommunications and other Legislation Amendment (Assistance and Access) Bill 2018.

I have attached my response to the Senate Standing Committee for the Scrutiny of Bills' Digest 12 of 2018, as requested in your correspondence.

Yours sincerely

PETER DUTTON 22/11/18

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Assistance regime – Schedule 1

1.61 The committee seeks the minister's detailed advice as to:

- **why it is considered necessary and appropriate to allow 'acts or things', other than those specified under proposed section 317E, to be specified under a technical assistance request, a technical assistance notice, and a technical capability notice (insofar as the acts or things are by way of giving help to ASIO or an interception agency);**
- **why it is considered necessary and appropriate to expand what constitutes 'listed help' by delegated legislation, and whether specific consultation obligations (beyond those in section 17 of the *Legislation Act 2003*) can be included in the bill in relation to a determination made under proposed subsection 317T(5) (with compliance with such obligations a condition of the validity of the legislative instrument);**
- **why it is considered appropriate that a request or notice may be issued in relation to the performance or exercise of a function or power relating to the enforcement of any criminal law (including any foreign criminal law) or law imposing any level of pecuniary penalty, noting that this would allow agencies to use the proposed framework in relation to very minor offence or breaches of the law;**
- **why it is considered appropriate to allow a technical assistance request to be issued (and therefore immunity given to providers) in relation to the performance or exercise of a function or power relating to the interests of Australia's 'foreign relations' or 'national economic well-being'; and**
- **the appropriateness of including in the bill a requirement that consultation with a provider be conducted prior to issuing a technical assistance notices, similar to the requirement under proposed section 317W in relation to a technical capability notice.**

<u>Necessity of specifying acts or things beyond listed 'acts or things' in section 317E</u>

Paragraphs 317E(1)(b)-(j) are exhaustive with respect to technical capability notices (TCN) and additional types of help may only be developed if set out in a legislative instrument determined by the Minister in accordance with subsection 317T(5).[1]

Paragraphs 317E(1)(a)-(j) are non-exhaustive with respect to technical assistance requests and technical assistance notices with the proviso that additional specified assistance is of the same kind, class or nature as those listed and that the assistance is connected to the eligible activities of the provider and related to the agency's functions.[2] This is set out in subsection 317G(6) for TARs and subsection 317L(3) for TANs.

The key rationale for not limiting the types of request is the need for operational flexibility in complex, technologically diverse, circumstances. There are many technical things that a provider may be able to do to appropriately assist law enforcement beyond the strict list of

[1] Explanatory memorandum, p38 para 54.
[2] Explanatory memorandum, p45 and p47.

activities in 317E. For example, disruption of a service being used for criminal activity may not directly be captured by 317E(1)(h) – (i) but would arguably be a thing of a similar kind to those activities. These kinds of disruptions are an often-used and necessary function of agency and telecommunication provider relationships and routinely occur through requests to domestic providers under section 313 of the *Telecommunications Act 1997*.[3] Notably, section 313 currently operates with a significantly higher degree of ambiguity than the proposed framework. A non-exhaustive application of the items in 317E will give greater specify to requests whilst maintaining the necessary flexibility and technological neutrality to ensure that measures remain useful in the rapidly changing communications environment.

As noted above the non-exhaustive nature of 317E does not extend to TCNs, which can require providers to build capabilities that go beyond business requirements. The non-exhaustive listed acts or things with respect to technical assistance requests (TAR) reflect the voluntary nature of requests. Providers have the ability to refuse any request they receive. Thus, where a provider is uncomfortable with the assistance they are being asked to provide, they may simply decline to answer a request. In this way, providers are protected from being required to provide kinds of assistance with which they take any issue under technical assistance requests. It is a requirement that providers be notified of the voluntary nature of these requests (see section 317HAA).

With respect to technical assistance notices (TAN), the non-exhaustive listed acts or things are limited by the fact that a TAN can only require a provider to do things they are already capable of complying. This limitation is reflected in the distinction between the language of TANs and TCNs, expressed in section 317T(2)(a) which requires a provider be '***capable** of giving listed help*' as opposed to '*giving help*' in 317L(2). The specification of things outside the listed acts or things in section 317E is then limited by the existing capabilities of the provider issued with the notice. Providers cannot be penalised for non-compliance with a notice which requires they provide an additional kind of assistance beyond those specified in section 317E where that assistance is not within their present ability (as requiring a provider to build a new capability or system would be covered by a TCN).

However, where a provider has the ability to offer assistance which falls beyond the precise words of the listed acts or things defined in section 317E – but is of a similar kind, class or nature – they may be called upon to provide this assistance under a TAN. The ability to compel these additional kinds of assistance is deliberate and in keeping with the rationale for the compulsory nature of TANs. Under subsection 317L(2), technical assistance notices may only be issued for the relevant objectives of enforcing the criminal law and laws imposing pecuniary penalties, assisting the enforcement of the criminal laws in force in a foreign country or safeguarding national security. These relevant objectives are sufficiently serious that providers should be compelled to offer any assistance that it is within their power to provide – so long as these kinds of assistance do not infringe the Bill's other limitations.

To assist the Committee, the table below outlines ways in which all the items at section 317E might be used to assist agencies.

[3] See *Balancing Freedom and Protection: Inquiry into the use of subsection 313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services,* Standing Committee on Infrastructure and Communications.

Operational examples from law enforcement agencies

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	- Requesting an ISP provide the password they have enabled on a customer supplied home modem to facilitate a review of its logs during a search warrant to identify connected devices. - Requesting a cloud storage provider changes the password on a remotely hosted account to assist with the execution of an overt account based warrant.
(b)	Providing technical information	- An application provider providing technical information about how data is stored on a device (including the location of the encryption key) to enable forensically extracted data to be reconstructed. - An international cloud hosted storage provider providing details of where a customer's data is hosted to enable a MLAT process to be progressed to the host country seeking lawful access. - A mobile device provider providing a copy of their WiFi AP location maps generated through bulk analysis of customers data to correlate with location records extracted during a forensic examination of a device.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	- Requesting a cloud service provider provide a copy of the contents of a hosted account in a particular format pursuant to the execution of an overt account based warrant. - Requesting that data held in a proprietary file format extracted from a device during a forensic examination pursuant to an overt search warrant is converted into a standard file format.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer	- Requesting a shared data centre provide access to customers computer rack to enable the execution of a computer access warrant or installation of a data surveillance device under warrant.

Sub section 317E(1)	Listed act or thing	Examples
	equipment, an electronic service etc.	
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	- Requesting that a social media platform assist with testing or development of a tool to automate the creation of online personas and historical content to facilitate online engagement.
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	- Requesting an ISP advise of any technical changes to their network which could impact on an existing interception.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	- Requesting a carrier increase the data allowance on a device that is subject to a surveillance device warrant to enable the surveillance device to be remotely monitored without consuming the targets data. - Temporarily blocking internet messaging to force a device to send the messages as unencrypted SMS's.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	- Requesting a carrier force a roaming device to another carriers network to enable the enhanced metadata collection capabilities of the new carrier to collect information pursuant to a prospective data authorisation.
(j)	An act or thing done to conceal the fact that anything has been done covertly in the	- Requesting that the provider not inform the customer of the assistance provided to enable a computer access warrant.

Sub section 317E(1)	Listed act or thing	Examples
	performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties; or - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	- Requesting that the provider delete an audit log in a customer's device relating to a computer access warrant. - Requesting a provider restore a password that was temporarily changed to enable a computer access warrant. - Requesting a provider allocate a specific dynamic IP address relating to remote access pursuant to a computer access warrant to conceal the access.

Operational examples from intelligence agencies

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	ASIO establishes physical access to a target's mobile phone and manages to acquire a copy of the phone's contents. The opportunity is rare and unique in that the target normally employs fairly good security awareness and tradecraft. Stored within the database of an application on the phone are historical conversations with other subjects of interest that indicate the group are in the initial stages of planning a mass casualty attack at an upcoming music festival. Unfortunately the copy of the phone's contents

Sub section 317E(1)	Listed act or thing	Examples
		only reveals a snapshot in time of the targets' intentions and ASIO cannot formulate an informed assessment of the group's intended activities. The application used by the group stores messages on a server in the cloud and makes use of various authentication mechanisms to authorise access to user accounts, limiting ASIO's ability to establish contemporary coverage of the group. On seeking appropriate warrants authorising ASIO to lawfully gain coverage of the target's communications, ASIO seeks out the designated communications provider (DCP) with capacity to deactivate the relevant authentication mechanisms allowing, ASIO to authenticate the target's account to provide up-to-date and ongoing coverage of the group's intentions and threat to Australia's security.
(b)	Providing technical information	In the example above, once ASIO overcomes the relevant protection mechanisms to access the relevant communications, without further technical assistance from the DCP, ASIO could expend significant time and resources attempting to understand the structure of the database associated with the chat application. The database may be complex with messages, parties to a conversation and associated attached media all stored in different portions of the database making an assessment of the subjects involved in the plan and their intentions quite difficult. It could take ASIO months to organise the data in a legible format. Using a Technical Assistance Notice, ASIO would seek out the DCP responsible for the application to gather technical information about how the application makes use of a database to store local copies of communications that have been sent and received by the application, enabling efficient and timely analysis of the relevant communications.
(C)	Installing, maintaining, testing or using software or equipment	An anonymous call is placed to the National security Hotline indicating that a Terrorist cell is planning a bombing attack against the SMH Fun run in Sydney. ASIO receives this tip-off just two

Sub section 317E(1)	Listed act or thing	Examples
		weeks before the event and only knows one of the group members involved. To avoid detection the group do not communicate via phone calls or face to face meetings but instead plan their attack online using application that encrypts messages as they are sent by users. Sent messages are received by the application's central server where they are decrypted and then re-encrypted with the intended recipient's key before being delivered to the intended recipient's device. ASIO secures an appropriate warrant and asks the communications provider to store copies of the target's communication before they are re-encrypted with recipient keys. To facilitate this, ASIO works with the DCP to install ASIO-controlled equipment that stores the communications. Interestingly, ASIO would store the communications in an encrypted format to prevent unauthorised access to the warranted material prior to it being disseminated back to ASIO.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	ASIO may require that information data obtained by a carrier in response to a warrant be provided in a format that is compatible with ASIO's systems and allows for appropriate analysis.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	Further to the example above, ASIO, in conjunction with the DCP, identifies a physical data centre that represents the best location to acquire copies of the target's unencrypted communications; however, the data centre is owned and operated by a third-party company. ASIO in conjunction with the chat application DCP work with the data centre DCP to arrange appropriate rack space, power and cabling for the ASIO server equipment.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	Further to the example above, ASIO assesses that any perceivable impact on the target's electronic service (the chat application) may result in an acceleration of the target's attack planning because ASIO assess the target exhibits a heightened level of paranoia, is erratic and prone to violence. ASIO works carefully with the DCP to ensure that the installed equipment has no

Sub section 317E(1)	Listed act or thing	Examples
		perceivable effects on the target's usage of the app and is entirely covert in its operation.
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	In the above example, the DCP intends to change the physical location of their infrastructure and notifies ASIO in advance of the change so ASIO can plan for the relocation of the ASIO equipment to ensure coverage of the target's communications is maintained.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	It's feasible, in the example above, that ASIO's work with the DCP, ensuring that the installed equipment has no perceivable effects on the target's usage of the application, could require some modification, or substitution of, characteristics of a service provided by the DCP – or indeed, substitution of the service itself - in order to ensure the ongoing covert nature of ASIO's operation.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties - assisting the enforcement of the criminal laws in	Further to the above example, it's also feasible that various other activities would be required to ensure the ASIO's operation remains covert, including: - Requiring that the assistance provided is kept confidential by the provider. - Asking the staff involved in providing the service to sign confidentiality agreements. - Requesting that a cover story to be adopted when explaining the nature of assistance being provided. - Adjusting billing, account access, data transfer logs etc. to hide evidence of access to a target device or service. - Facilitating covert physical access to a facility.

Sub section 317E(1)	Listed act or thing	Examples
	force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	

Expansion of what constitutes 'listed help' by delegated legislation

The Minister under subsection 317T(5) has the power to expand the definition of 'listed help' by legislative instrument. Legislative instruments were deemed the correct avenue to expand this definition because this will allow the powers of TCNs to be readily and quickly adapted. The communications industry is one of the world's most dynamic, and it is important that law enforcement and security agencies retain the ability to combat crime and national security threats notwithstanding advances in technology.

Section 317T(6) provides that, in making a decision to add an item to the definition of listed help in section 317E by legislative instrument, the Minister must consider – at section 317T(6)(d) – the likely impact of the determination on designated communication providers. The Minister must also consider the objectives of the *Telecommunications Act 1997* (Telecommunications Act), which goes to the competitiveness of the telecommunications industry and innovation in that industry. While the Minister is not required to consult with providers in making their determination, it could be fairly stated that consultation would be a necessary step for the Minister to have due regard to the required matters. Further, the legislative instrument will be subject to parliamentary scrutiny as part of the disallowance process.

Ability to use requests or notices to investigate minor offences

The relevant objectives for which requests and notices may be issued are limited to, among other things, enforcing the criminal law and laws imposing pecuniary penalties and assisting the enforcement of criminal laws in force in a foreign country. While these objectives are theoretically wide enough to allow law enforcement to pursue minor criminal offences, practical and investigative limitations will prevent such an outcome. The powers that these notices are expected to be most usefully deployed in support of include interception and surveillance device warrants under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and *Surveillance Devices Act 2004* (SD Act). Generally the use of these underlying powers require the investigation of a serious criminal offence attracting three or more years maximum imprisonment (seven for interception warrants).

The wording of the relevant objectives also reflects the purposes for which authorisations for telecommunications data may be made under Chapter 4 of the TIA Act. Data authorisations are a critical law enforcement power and widely used to investigate serious offences and to access exculpatory evidence; as the data does not go to the content of a communication it is generally taken to be a less privacy intrusive power. It is important to align the purposes for which the new measures may be used with the thresholds for access to data, as the measures are designed to complement existing, and appropriately safeguarded, functions of agencies (particularly when these powers interact with the communications environment).

Furthermore, these objectives are consistent with the Telecommunications Act, which sets out at section 313 the purposes for which a carrier or carriage service provider may be compelled to give such help as is reasonably necessary. These purposes include enforcing the criminal law and laws imposing pecuniary penalties, assisting the enforcement of the criminal laws in force in a foreign country, protecting the public revenue and safeguarding national security. With the removal of protecting the public revenue during consultation and the additional safeguards applied to the regime (see section 317ZG and decision-making criteria, for example) the relevant objectives available to enliven the power to issue a notice under the present legislation are in effect narrower than those purposes required to exercise analogous powers available in the Telecommunications Act.

Fiscal responsibility measures in overarching governance legislation means that agencies will be highly unlikely to be able to deploy resources to target minor crimes. The requirement under subsection 317ZK(3) that providers be compensated for the reasonable costs of compliance by the issuing agency means that these powers will be exercised sparingly and in light of budgetary constraints.

The reference to 'pecuniary penalties' in these provisions is not intended to encompass small-scale administrative fines. In Commonwealth, State and Territory legislation there are significant pecuniary penalties for serious breaches of the law, particularly laws regarding corporate misconduct and these crimes may be a legitimate target for investigation with industry assistance – this purpose is outlined in the explanatory memorandum.

'Interests of foreign relations' and 'Australia's national economic well-being' as reasons to issue a technical assistance request

The wider remit to issue a TAR, beyond the relevant objectives available to issue either a TAN or TCN, reflects the voluntary nature of the requests. These provisions provide a foundational framework for voluntary assistance which clearly indicates on what basis that assistance can occur. This means that providers can ultimately decide if they are willing to provide assistance in accordance with the relevant objective of the request.

The reference to interests of Australia's foreign relations and or Australia's economic well-being in new subparagraph 317G(5)(d) reflects the functions of Australia's intelligence and security agencies (this subparagraph also refers relevantly to national security) as set out in the section 11 of the *Intelligence Services Act 2001*. It is intended to support voluntary technical assistance requests made by Australia's intelligence and security agencies. It is not intended to support voluntary assistance requests made by interception agencies.

Once again, these objectives are consistent with the Telecommunications Act which sets out at section 313 the purposes for which a carrier or carriage service provider may be

compelled to give such help as is reasonably necessary. These purposes include, among others, assisting the enforcement of the criminal laws in force in a foreign country and protecting the public revenue. The language of the present legislation, by contrast, provides at subsection 317G(5) relevant objectives for issuing a technical assistance request include the interests of Australia's national security and the interests of Australia's national economic well-being. Despite these similarities, the power conferred by subsection 317G(5) is weaker than that at section 313 of the Telecommunications Act as the former section does not confer any power to compel conduct but merely to ask for assistance.

The rationale for granting civil immunity to providers for complying with a TAR issued in the interests of Australia's foreign relations or the interests of Australia's national economic well-being is the same as the rationale for the immunity under other relevant objectives of enforcing the criminal law and laws imposing pecuniary penalties and assisting the enforcement of the criminal laws in force in a foreign country. Where a provider is asked to provide assistance and does so, or attempts to do so purportedly in good faith, they should not be at risk of accruing civil liability as a result. Furthermore, these immunity provisions are consistent with the circumstances in which a carrier or carriage service provider may be granted civil immunity under section 313(5) of the Telecommunications Act for compliance with an obligation to provide reasonable assistance. It is important to note that proposed provision does not provide immunity from criminal liability.

Lack of section 317W consultation when issuing a technical assistance notice

Although there is no explicit consultation process for decision-makers to undergo before issuing a TAN, the practical effect of the legislation would require consultation in most cases before a notice is given to a provider. A decision-maker must be satisfied that the requirements imposed by a notice are reasonable and proportionate and that compliance with the notice is practicable and technically feasible.

As changes made as a result of public feedback make clear, in deciding whether a notice is reasonable and proportionate, the decision-maker must have regard to the interests of the relevant provider, the availability of other means to achieve the notice and the privacy and cybersecurity expectations of Australians (proposed sections 317RA and 317ZAA explains). These changes were made in response to public feedback for further clarification on the standards of reasonableness and proportionality (explained in detail in the Explanatory Memorandum)[4] and suggestions that a TAN should have a consultation component.

In most circumstances, it would be expected that a decision-maker would need to consult with the provider in order to determine if the assistance requested is reasonable, proportionate, practical and technically feasible. For example, noting the technical nature of requirements in a notice, a decision-maker is unlikely to be satisfied of their technical feasibility without having a prior understanding of a provider's system infrastructure and capabilities – information that would have to be gained through consultation with a provider.

This framework mimics, in part, how consultations currently occur through section 313 of the Telecommunications Act. Agencies will typically engage early with a provider about possible requirements and the outcome on an eventual request reflects a negotiation between both parties.

[4] See Explanatory Memorandum pp. 48-9

1.66 The committee requests the minister's detailed explanation of why it is considered appropriate to exclude judicial review under the *Administrative Decisions (Judicial Review) Act 1977* in relation to decisions made under proposed Part 15 (industry assistance) (noting that it is already possible to prevent the disclosure of sensitive information by excluding classes of decisions from the requirement to provide reasons under the ADJR Act).

Appropriateness of excluding review under the ADJR Act

The exclusion of judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (AJDR Act) is consistent with the approach to review for similar types of decisions made under the *Intelligence Services Act 2001* (IS Act), *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act). This exclusion reflects the serious circumstances in which these powers are used and the need for timely execution.

As detailed in the explanatory memorandum, TANs may be issued in the course of an ongoing and evolving investigation and it is imperative that such a notice can be issued and used quickly. A review process under the ADJR Act could adversely impact the effectiveness and outcomes of an investigation. Decisions to issue technical capability notices are further unsuitable for the judicial review process provided by the ADJR Act because they are made by the Attorney-General and are ministerial decisions to develop law enforcement and national security capabilities.

In the event a provider wishes to seek judicial review of any administrative decision to issue a notice, there are a number of grounds for challenging the decision as well as specific defences. For example, a defence to enforcement is available where compliance with a notice would contravene a law of a foreign country. By way of example, a TAN or a TCN can be challenged if it were deemed to create broad vulnerabilities in a network or where it is infeasible that the decision-maker could have considered the requirements of the TAN or TCN to be reasonable or proportionate. Accordingly, judicial review is available for decisions under this Schedule. The *Judiciary Act 1903* and the Constitution provide avenues for review in the High Court, Federal Court and State Supreme Courts, depending on the source and nature of the request.

Both an affected person, and a provider on behalf of an affected person would have standing to challenge unlawful decision making. While this may not be appropriate during an investigation, the admissibility of evidence that is gained by operation of this Bill's powers and that is later tendered in a criminal proceeding could be challenged if it was unlawfully or improperly obtained. The right to an effective remedy therefore remains available.

The industry assistance framework of Part 15 of the present legislation is designed to incentivise cooperation with industry; providing a regime for the Australian government and providers to work together to safeguard the public interest and protect national security. In the unlikely event that enforcement action is required, applications for enforcement under new Division 5 of Schedule 1 will be considered independently by the Federal Court or the Federal Circuit Court.

1.71 The committee requests the minister's advice as to why it is considered necessary and appropriate to provide immunity from civil liability to designated communications providers with respect to any act or thing done in accordance or

compliance with a technical assistance request, technical assistance notice or a technical capability notice (noting that the acts or things that may be specified under a request or notice are not exhaustively set out in the bill).

Necessity and appropriateness of granting providers civil immunity

New subsection 317ZJ(1) provides designated communications providers immunity from civil liability for, or in relation to, any act or thing done in compliance, or in good faith in purported compliance, with a TAN or TCN. It is full immunity for civil actions brought under Commonwealth law.

As detailed in the explanatory memorandum[5], 'purported compliance' means that providers are not liable to an action or other proceeding in the exceptional circumstances where some elements of a TAN or TCN are deemed invalid. A provider acts in good faith if the provider acts with honesty according to the standards of a reasonable person.

Complying with a TAN or TCN (or acting in accordance with a TAR) may involve disclosure of the development of a new service or technology in violation of general intellectual property laws or a provider's contractual obligations. Where a provider is asked to provide assistance and does so, or attempts to do so purportedly in good faith, they should not be at risk of accruing civil liability as a result. These immunity provisions, including ones for TARs in 317G(1)(c) – (d), are consistent with the circumstances in which a carrier or carriage service provider may be granted civil immunity under subsection 313(5) of the Telecommunications Act for compliance with an obligation to provide reasonable assistance.

Where a provider is given civil immunity for an act or thing which was not expressly defined in the list of acts or things under section 317E, this activity will necessarily have been one of the same kind, class or nature of the existing listed acts or things. Any additions to the existing list must be set down by the Minister in a legislative instrument with reference to the criteria set out by 317T(6). This ensures that civil liability is only granted for activities where regard has been had to the implications for privacy and the interests of law enforcement, national security or other salient concerns.

1.76 As the explanatory materials do not address this issue, the committee requests the minister's advice as to why it is proposed to use offence-specific defences (which reverse the evidential burden of proof) in this instance. The committee's consideration of the appropriateness of a provision which reverse the burden of proof is assisted if it explicitly addresses relevant principles as set out in the *Guide to Framing Commonwealth Offences*.

Appropriateness of reversing the onus of proof for disclosure offences

The Government considers it is appropriate to create offence-specific defences to protect sensitive information where the information is in the hands of entrusted persons such as those covered by paragraph 317ZF(1)(b). These persons bear an additional level of responsibility over ordinary citizens and it is reasonable to expect they exercise due care in their handling of technical information and be able to show that, where they have disclosed information, they have done so for an authorised purpose.

[5] Explanatory memorandum, p69 para 272.

This offence is consistent with the drafting of similar disclosure offences such as the use and disclosure offences contained in Division 6 of the TIA Act. The defences to the disclosure of information offences, such as section 181A(3) TIA Act, are offence-specific defences similar to that of the proposed legislation. Given the similar material protected by these offences, the proposed offence-specific defences of section 317ZF are appropriately drafted.

"Authorised disclosure" is an offence-specific defence to the offence. Where a defendant wishes to raise this defence in a prosecution concerning an offence of authorised disclosure, the evidentiary burden will be on the defendant to show that the disclosure was authorised.

The Attorney-General's Department's *A Guide to Framing Commonwealth Offences, Infringement notices, enforcement provisions* sets out the circumstances where an offence-specific defence may be appropriate where a matter is "*peculiarly within the knowledge of the defendant*" and "*significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter*".[6]

The unauthorised disclosure offence within Schedule 1 meets these criteria. Rather than require the Crown to prove this offence, relevant persons[7] covered will be best-placed to make out a valid defence. The facts required to prove this defence will be readily provable as a matter peculiarly within the knowledge of these individuals or to which they have ready access. That is, it is peculiarly within the ability of the relevant individuals to rebut the allegation of unauthorised disclosure.

1.82 The committee requests the minister's more detailed advice as to:

- **the circumstances in which it is considered it would not be appropriate to compensate a provider that is subject to a technical assistance notice or technical capability notice;**
- **why (at least high-level) guidance as to the circumstances in which proposed section 317ZK will not apply cannot be included in the bill.**

<u>Circumstances in which it would not be appropriate to compensate a provider</u>

Section 317ZK sets out the terms and conditions on which help is to be given etc. New section 317ZK applies if a person is required to provide help under new technical assistance notice or technical capability notice issued in accordance with new sections 317L and 317T, respectively.

As stated in the explanatory memorandum, new subsection 317ZK(3) states that, generally, compliance with requirements is on a no profit or loss basis. New paragraph 317ZK(3)(b) notes that the provider is not expected to bear the reasonable costs of complying with a requirement.

However, in limited circumstances, it may be appropriate that the costs of complying with a new TAN or TCN are not recoverable. New subsections 317ZK(1) and (2) create a public

[6] Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and enforcement provisions*, pg. 50.

[7] Persons in this sense means those included under proposed section 317ZF(1)(b) and includes, for example, a designated communications provider or an officer of an interception agency.

interest exception where the Director-General of Security or the chief officer of an interception agency is satisfied it would be contrary to the public interest for a notice to be settled in accordance with the terms and conditions in subsections 317ZK(3) and (4). This power is envisioned as operating in limited circumstances where it is prudent to protect public money from unscrupulous providers or providers who cause damage through negligence.

As noted by the Committee, the Explanatory Memorandum provides the language of 'reckless and wilful' to guide decision-makers. New subsection 317ZK(2) sets a high threshold where the decision-maker should be satisfied that waiving the established compliance processes is in the public interest, and turn their mind to a range of commercial, law enforcement and security considerations.

Section 317ZK also introduces safeguards to bound the power of a decision-maker not to compensate a provider. As the committee has noted, subsection 317ZK(15) invalidates any notice that amounts to an acquisition of property on other than just terms. Additionally, any decision made not to compensate a provider under section 317ZK will be eligible for judicial review under the *Judiciary Act 1903*.

Why guidance to non-application of 317ZK is not included in the Bill

The Government considers it inappropriate to provide guidance within the legislation other than what is already identified as part of subsection 317ZK(2). The range of commercial, law enforcement and security considerations identified provide sufficient scope for decision makers to consider a broad range of circumstances to ensure that cases are considered on an individual basis.

The Government may consider implementing the language of recklessness or wilful actions into the text of the legislation where this is likely to better contextualise the public interest test.

Computer access warrants – Schedule 2

1.87 The committee requests the minister's advice as to why it is considered necessary to allow for the delegation of ASIO's authority in relation to the concealment of activities undertaken under certain warrants to 'any person' or class of persons, and the appropriateness of amending the bill to provide some legislative guidance as to the categories of people to whom those powers might be delegated.

Necessity of allowing ASIO to delegate concealment powers

The addition of subsections 25A(8), 27A(3C) and 27E(6) to the list of purposes for which power may be delegated to exercise authority under warrant is consistent with the existing purposes under which power may be delegated. Given the need to conceal activity under a computer access warrant, delegating power to someone with actual access may be necessary to ensure activities remain covert where ASIO no longer has access to the computer or computer system on which the warrant was executed.

The Government considers it may not be appropriate to amend the Bill to provide some legislative guidance on the aforementioned categories of people to whom those powers

might be delegated. This is primarily due to the fact that it is more appropriate for ASIO's delegation powers to be determined by ASIO, which should already be entrenched in either policy or statutory authority. It may not be appropriate to establish and potentially curtail any delegation powers that could otherwise be afforded by ASIO, which already currently affect the operation of Computer Access Warrants contained under Schedule 2 of the Bill.

The Inspector-General of Intelligence and Security has extensive oversight of ASIO activities, including those things authorised under the relevant warrants.

1.121 The committee seeks the minister's detailed advice as to:

- **why the categories of persons eligible to issue computer access warrants should not be limited to persons who hold judicial office;**
- **the appropriateness of lowering the threshold for ASIO to access intercepted communications, noting that administrative convenience is not generally an acceptable basis for doing so;**
- **why it is necessary and appropriate to enable law enforcement officers to access computer data without a warrant in certain emergency situations (noting the coercive nature of these powers and the ability to seek a warrant via the telephone, fax or email);**
- **the appropriateness of retaining information obtained under an emergency authorisation that is subsequently not approved by a judge or AAT member;**
- **the appropriateness of enabling ASIO and law enforcement agencies to act to conceal any thing done under a warrant *after* the warrant has ceased to be in force, and whether the bill could be amended to provide a process for obtaining a separate concealment of access warrant if the original warrant has ceased to be in force;**
- **the effect of Schedule 2-5 on the privacy rights of third parties and a detailed justification for the intrusion on those rights, in particular:**
    - **why there is no requirement that a person executing a computer access warrant must first seek the consent of the occupier or, at a minimum, announce their entry, before entering third party premises;**
    - **why proposed paragraph 27E(2)(e) (and identical provisions in Schedules 3-4) does not specifically require the judge or nominated AAT member to consider the privacy implications for third parties of authorising access to a third party computer or communication in transit;**
    - **why proposed subsection 27E(5) (and identical provisions in Schedules 3 and 4) does not include a prohibition on 'copying' of third party data, or at a minimum, a requirement that copies of any third party data be destroyed if it contains no relevant investigative value;**
    - **why it is necessary to authorise relevant law enforcement officers to use a computer found in the course of a search or a telecommunications facility or other electronic equipment for the purpose of obtaining 'account-based data' in relation to any person who uses or has ever used the relevant computer;**
    - **the necessity for the definition of 'account based data' to include the data of potentially innocent third parties who have links with an individual who is the subject of a search warrant;**
- **why it is necessary and appropriate to enable a law enforcement officer to obtain a computer access warrant simply to 'determine' whether a control**

order has been complied with, when breach of a control order is an offence and, as such, there is already a power for the officer to obtain a warrant when there is a reasonable suspicion that an offence is being or is likely to be committed;

- **why it is necessary and appropriate to allow the use of information obtained under a computer access warrant that was granted on the basis that an interim control order was in force in circumstances where the control order is subsequently declared by a court to be void.**

Categories of people able to issue computer access warrants

The addition of new subsection 28(1A) to the SD Act allows law enforcement officers to apply to appropriate authorising officers instead of seeking authorisation from a Judge or nominated Administrative Appeals Tribunal (AAT) member in certain emergency situations.

The use of emergency authorisations for the use of surveillance devices is not new. Since 2004, emergency authorisations have been available for the broader set of surveillance device powers under the SD Act. Emergency authorisations are available only in very limited circumstances, namely where there is imminent risk of serious violence or substantial property damage, where it will assist relating to a recovery order, and where there is a risk of loss of evidence. In each of these circumstances, the use of an emergency authorisation must be immediately necessary to achieve the stated purpose, and must demonstrate that it is not practical to apply for a Computer Access Warrant (CAW). In practice, emergency authorisations are only utilised rarely. For example, in the *Surveillance Device Act Annual Report 2016-2017*, no law enforcement agencies made an emergency authorisation.

Various safeguards exist to ensure that emergency authorisations are necessary and proportionate. Within 48 hours after an emergency authorisation is given by an authorising officer, there must be an application to an eligible Judge or AAT member for approval. In deciding whether to approve this application, an eligible Judge or AAT member must, being mindful of the intrusive nature of the use of a surveillance device, consider various things, such as urgency in relation to the stated purpose (e.g. risk of serious violence to a person), alternative methods, and whether or not it was practicable in the circumstances to apply for a surveillance device warrant.

Information gathered as part of an emergency authorisation is considered ‘protected information’ and is subject to the strict use and disclosure provisions that ordinarily exist for information obtained from powers exercised under the SD Act. Criminal liability is attached to unauthorised disclosure of information protected under the SD Act.

The availability of the use of computer access powers under an emergency authorisation is proportionate and is necessary to ensure that, in special circumstances, the computer access powers can be used for the purposes of public safety and national security. The Government views these powers as balancing the interests of the public and recognition of the importance of privacy of the Australian community.

Appropriateness of lowering threshold for ASIO to access intercepted communications

Computer access capabilities do not work in a vacuum and may require some interaction with the telecommunications network. As a consequence, it may be necessary to use interception capabilities in order to technically enable computer access. The TIA Act has been amended in order to provide for this incidental interception. Importantly, the interception of communications is only permitted insofar as it is necessary to execute the computer access warrant (see Schedule 2, Item 6 for example).

In effect, this is not lowering the threshold for interception as the amendments do not permit interception independently. This is consistent with the general exceptions to the prohibition against interception in section 7 of the TIA Act. Subsection 7(2) exempts a number of legitimate activities that require the incidental interception of communications from the prohibition, including 'the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO employee, in the lawful performance of his or her duties' for the purposes of detecting whether a listening device is being used.

The stated objective of this measure is two-fold: to enhance the operational effectiveness of the use of a computer access warrant (both existing ASIO warrants and new warrants under the SD Act) and to ensure that multiple warrants are not required to achieve a single purpose – that being the execution of a CAW. If law enforcement agencies and ASIO had to meet the thresholds for the existing interception regime may also mean that a CAW cannot be executed, or significant delay imported into the process. We note that the threshold to obtain a CAW will be offences with a maximum period of 3 years' imprisonment or more in most instances. The existing threshold for interception warrants is generally offences with a maximum 7 years' or imprisonment.

Delay, or inability, may result in either significant loss of evidence or the continuation of serious crime. The Government views that incidental interception is rationally connected to computer access and is a necessary, proportionate and reasonable measure to ensure available judicially approved powers can actually be executed.

Appropriateness of retaining information obtained in an emergency without subsequent judicial approval

Where information is obtained in the course of an investigation, including as part of an emergency authorisation, it is paramount that said information can be retained if it has investigative value. The drafting of subsection 35A(6) which permits the retention of evidence obtained without a valid emergency authorisation reflects existing subsection 35(6) in the SD Act. While this evidence is improperly obtained, it may be critical for valid investigations into serious crime as detailed in subsection 45(5). Existing section 36 in the SD Act also provides that evidence obtained under an emergency authorisation which has subsequently been approved by an eligible Judge or nominated AAT member will be admissible in any proceedings. Thus, the fact that the evidence was obtained under an authorisation prior to receiving approval does not render such evidence inadmissible.

Information gathered as part of an emergency authorisation is considered 'protected information' and is subject to the strict use and disclosure provisions that ordinarily exist for information obtained from powers exercised under the SD Act. Criminal liability is attached to

the unauthorised disclosure of 'protected information' and this is another means by which the privacy rights of individuals will be protected.

Appropriateness of enabling ASIO to conceal warranted activities after warrant expiry

The Committee specifically raises the issue of the proposed concealment powers under the existing ASIO CAW regime. However, the Bill provides concealment powers for both law enforcement and ASIO. The rational for both remains the same. Undertaking surveillance activities on an electronic device may alter data, or leave traces of activity, on that device. This may allow for suspects to recognise the lawful intrusion by law enforcement agencies and effectively change the way they communicate for the purposes of avoiding law enforcement (e.g. recognition may lead to reverse engineering the police capabilities and methodology leading to individuals avoiding certain technologies or undertaking counter-surveillance activities). Accordingly, the concealment of the execution of a CAW is vital to the exercise of the powers under Schedule 2, and indeed, the existing powers under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). This is also a practical measure acknowledging that ASIO might not necessarily be able to access while a warrant is in place to undertake concealment activities.

In the event that law enforcement agencies and ASIO not being able to conceal, there is significant risk to the exposure of police technologies and methodologies. This could reduce opportunities for agencies to prevent the commission of crimes. The Government views there is a clear rational connection between the availability of concealment provisions both under this Bill and within the ASIO Act and the necessary pursuit of public safety, public order and national security.

The measures are subject to limitations, safeguards and oversight mechanisms designed to ensure that the proposed and existing measures are used proportionately, reasonably and only as necessary. For example, the proposed CAWs under the Bill are subject to the requirement for judicial authority and oversight be the Commonwealth Ombudsman, and the existing ASIO CAWs are subject to ministerial oversight (approval required by the Attorney-General) and oversight by the IGIS.

Justification for the effect of schedule 2-5 on privacy rights of third parties

Lack of requirement to alert occupier before executing warrant

In line with the covert nature of surveillance, it would in many circumstances not be appropriate to notify a third-party before the execution of a CAW could take place. Indeed, there may be significant risks to capabilities and methodology, and risks to operations, if third-parties were required to be notified. The relationship between the third-party and the suspect, or the risk that the third-party poses to law enforcement operations may not be easily determined in the time necessary to execute the warrant.

The power for an eligible Judge or AAT member to authorise law enforcement entering a third-party premises for the purposes of executing a warrant is not a new concept to the SD Act or indeed other search warrants. For example, section 18 of the SD Act permits the authorisation of law enforcement entering '*other premises adjoining or providing access to*

premises'.[8] This highlights the necessity that surveillance activities may have to utilise third-party premises to execute surveillance warrants.

Section 27E will permit an eligible Judge or nominated AAT member to authorise law enforcement to enter third-party premises to execute the warrant. Importantly, the access to the third-party premises must be considered by the Judge or AAT and as such it is pre-authorised by an independent party and not at the discretion of the executing officer. These considerations must bear in mind privacy, the gravity of the offence and the availability of alternative measures to achieve the requisite access. Accordingly access will be appropriately constrained to meet the decision-making requirements of independent third-parties.

This access will also be subject to addition safeguards such as oversight by the Commonwealth ombudsman or IGIS (in respect of ASIO). Accordingly, the Government views that the inherent covert nature of surveillance necessitates the ability to access third-party premises where it is necessary to successfully execute a warrant, including for the purposes of concealing that execution.

Lack of requirement to consider privacy implications for third-parties

For the purposes of executing a warrant, a Judge or nominated AAT member may authorise activities which impinge on the privacy of third-parties. As this authority forms part of the broader warrant, the privacy interests of the affected third-parties will have had to have been considered by the Judge or nominated AAT member under paragraph 27C(2)(c) which requires consideration of the extent to which the privacy of any person is likely to be affected.

Lack of prohibition on copying third-party data

The copying or deletion of a third-party's data is permissible under a computer access warrant only where:

- It would be evidentiary material which may be obtained as part of the execution of the warrant and that third-party data is evidence of a crime (subject to use and disclosure rules); or
- It is necessary for both the execution, and concealment, of a CAW.

An integral part of executing a CAW may be inserting data or a program which may appear to be pre-existing data on the device. Prohibiting the ability to copy information, including third-party data, may critically hinder the ability to then replace that data again to conceal the execution of a CAW.

As acknowledged above, the eligible Judge or nominated AAT member must have regard to a range of factors, including the extent to which privacy of any person is likely to be affected, and whether there are any alternative means of obtaining the evidence or information sought to be obtained. Accordingly, law enforcement will need to provide as part of their application to the eligible Judge or nominated AAT member an assessment of privacy implications, including where that may impact third-parties. Notwithstanding, it may be impossible to

[8] Section 18 specifically relates to '*surveillance devices'* and may refer to physical surveillance device capabilities being used on adjoining property.

determine at the outset whose privacy may be impacted, especially where concealment of the execution of a CAW is concerned. Retaining as much flexibility as possible whilst ensuring that activities are reasonably necessary is paramount.

The Commonwealth Ombudsman, or IGIS (with respect to ASIO) will be a key oversight mechanism in the use of these powers. It will be within the purview of those agencies to critically consider agencies' copying of any third-party data and subsequent use. The Government views that the ability to copy third-party data under a CAW is appropriate and acknowledges the operational realties of executing highly technical capabilities such as those employed in CAWs.

Why it is necessary to authorise relevant law enforcement officers to use a computer found in the course of a search or a telecommunications facility or other electronic equipment for the purpose of obtaining '*account-based data*' in relation to any person who uses or has ever used the relevant computer

Amendments to the *Crimes Act 1914* will ensure that accessing a computer or data storage device under a search warrant permits the executing officer or a constable assisting to use that computer or data storage device – or any other equipment – for the purpose of obtaining access to account-based data.

Account-based data in relation to a person includes data associated with an account for an electronic service with end-users that is held by the person. This could be data associated with an email service, a Facebook account, an Instagram account, a Reddit subscription, a Twitter profile, a log-in to a commentary section on a news website or messaging services such as WhatsApp, Signal, and Telegram.

This modernises current search warrant powers under the respective acts and acknowledges that this is information which may be easily accessible and have evidentiary value from computers, data storage devices, or other equipment, during the execution of search warrants. Increasingly, persons that want to commit, or are committing serious crimes, utilise services out of convenience that may not necessarily be easily accessible through processes such as mutual legal assistance. For example, where a laptop computer is identified as holding critical data which identifies an email service associated with serious crime, the Government views that law enforcement and border force officers should be not be prevented from examining that account-based data for evidentiary purposes.

The transient and mobile nature of cloud communications requires law enforcement to access a range of data associated with the use of a particular computer. If a computer subject to the warrant is obtained, it is feasible that a broad range of persons may have been using that computer to conduct illicit activity, or that a person of interest is using the accounts of others to conduct illicit activity. The ease of online access makes strict account associations impracticable.

This power does not compel a person to assistance in accessing that laptop computer. It simply authorises police officers to access it (including remotely) where possible to do so (such as an unlocked laptop computer). Other powers such as assistance orders under section 3LA of the *Crimes Act 1914* (Crimes Act) will be required to compel a person to provide access, if necessary.

The necessity for the definition of 'account based data' to include the data of potentially innocent third parties who have links with an individual who is the subject of a search warrant

The definition of account-based data is focused on a particular person. Generally the account-based data will relate to data associated to an account for an electronic service which is related to the person of interest.

However, the definition also applies to account-based based data in relation to the person of interest which is associated with an account for an electronic service with end-users that is used or is likely to be used by the person. As identified in the explanatory memorandum, this may include data associated with an account held by another person (such as a family member, friend or business associate) but utilised by the person of interest. This recognises that persons of interest may utilise accounts held by another person to commit serious crime and goes to transient nature of cloud communications as discussed above.

Necessity and appropriateness of enabling law enforcement to determine compliance with a control order

A control order computer access warrant is a CAW that may be applied for by a law enforcement officer if a control order is in force and he or she suspects that access to data held in a computer would be likely to substantially assist in either protecting the public from a terrorist act, preventing the provision of support for a terrorist act or a hostile activity, or determining whether the control order is being complied with. In order for a control order computer access warrant to be granted, the law enforcement officer applying for the warrant, and the issuing Judge or AAT member, must be satisfied that there is a rational connection between the stated legitimate objective of the measure (e.g. protection of the public from a terrorist act), and the use of a computer access warrant being likely to substantially assist in achieving that objective.

Australia continues to face a serious terrorist threat which has seen an increased operational need to protect the public from terrorist acts. It is imperative that law enforcement be able to readily determine if a control order is being complied with. To this end, it is necessary and appropriate that special provision to determine compliance with a control order is a basis for issuing a computer access warrant beyond the general ability of law enforcement to obtain a warrant for such a purpose.

The use of surveillance device powers for the purposes of monitoring compliance with control orders is not a new concept. In 2016, the Australian parliament approved the use of surveillance device capabilities through the passing of the *Counter-Terrorism Legislation Amendment Act (No. 1) 2016*.

Necessity and appropriateness of allowing information obtained under a subsequently void control order to be used

Evidence gathered under a computer access warrant authorised to determine if the conditions of an interim control order, which is subsequently declared void, are being complied with may be admitted as evidence in specified circumstances. These

circumstances are limited to proceedings necessary to assist in reducing or preventing the risk of serious offences such as the commission or a terrorist act, causing serious harm to a person or serious property damage.

The Government considers it necessary and appropriate to ensure evidence generated by a subsequently void control order is admissible given the likelihood that such evidence will prove serious offences. Computer access warrants are uniquely suited to investigating clandestine communications, and thus more likely to provide evidence relating to serious terrorism offences. Additionally, this evidence may be required to prove offences against other members of a terrorist network. Evidence useful for proving serious offences against the individual targeted by the interim control order or their associates may be discarded if the voiding of an interim control order renders all evidence gathered during that investigation inadmissible in all circumstances.

This is consistent with the existing kinds of evidence which may be admitted to prove serious offences under subsection 65B(1) of the SD Act, in particular subparagraph 65B(1)(a)(i) which provides for control order warrants issued on the basis of an interim control order. The inclusion of computer access warrants issued to determine compliance with a control order in this list is commensurate with the existing items listed and a failure to extend this list to this new kind of warrant would be an oversight.

1.133 As the explanatory materials do not address, or do not adequately address, these issues, the committee requests the minister's detailed advice as to:

- **why it is considered necessary and appropriate to expand the circumstances in which evidentiary certificates may be issued under the *Australian Security Intelligence Organisation Act 1979* and the *Surveillance Devices Act 2004* to include the matters identified above;**
- **the circumstances in which it is intended that evidentiary certificates would be issued, including the nature of any relevant proceedings, and**
- **the impact that issuing evidentiary certificates may have on individuals' rights and liberties, including on the ability of individuals' to challenge the lawfulness of actions taken by law enforcement agencies.**

<u>Necessity and appropriateness of expanded power to issue evidentiary certificates</u>

The *Guide to Framing Commonwealth Offences, Infringement notices, enforcement provisions* notes that evidentiary certificates should generally only be used to settle formal or technical matters of fact that would be difficult to prove by adducing admissible evidence. It is generally unacceptable for evidentiary certificates to cover questions of law, which are for the courts to determine.

Amendments to the ASIO Act - Evidentiary certificate concerning voluntary assistance

Under the Bill, the Director-General may give a certificate in writing certifying one or more facts relevant to the question of whether he or she was satisfied that particular conduct relating to voluntary assistance to ASIO was likely to assist ASIO in the performance of its functions.

Certificates are to be prima facie evidence of the matters stated within the certificate (that is, certificates issued under the regime will be persuasive before a court, as distinct from a

conclusive certificate that cannot be challenged by a court or a defendant). The evidentiary certificate would only deal with factual matters, being the factual basis on which the Director-General reached his or her belief, and would not deal with questions of law that would be properly the role of the courts to determine.

Amendments to the ASIO Act - Concealment activities

Amendments will also be made to the ASIO Act which enable evidentiary certificates to be issued under section 34AA in relation to acts done by, or behalf of, or in relation to ASIO in connection with any matter in connection with a CAW. These evidentiary certificates will be prima facie evidence of matters stated within the certificate. The existing regime under section 34AA of the ASIO Act is framed to ensure that an evidentiary certificate will only cover the manner in which the evidence was obtained and by whom but not the evidence itself. As such, the court will retain its ability to test the veracity of evidence put before it.

For operational security reasons, the proposed regime does not provide a conclusive list of the facts that the Director-General or a Deputy Director-General may include and is not intended to provide a means for the prosecution to provide proof of any ultimate fact, or any fact so closely connected certificate. The regime is not intended to provide a means for the prosecution to provide proof of any ultimate fact, or any fact so closely connected with an ultimate fact so as to be indistinguishable from it, or facts that go to elements of the offence, without recourse for the course or the defendant to challenge the certificate and the facts it covers.

Amendments to the SD Act

The proposed evidentiary certificates within the SD Act relate to the protection of capabilities and methodology. In particular, there should be protections which go to mere technical manners in which evidence was obtained and by whom but not the actual evidence itself. These certificates will be prima facie. Evidentiary certificates will protect capabilities by largely preventing prosecutors from being required in the first instance to disclose the operation and methods of law enforcement unless a defendant seeks to dispute the veracity of the methods used to gather evidence against their interest.

Evidentiary certificates for the purpose of protection of capabilities and methodology already exist in Commonwealth legislation. For example, evidentiary certificates exist under the TIA Act for both actions taken by law enforcement and carriers.

The Government views that evidentiary certificates are necessary aspects of these regimes. Given the prima facie nature of the evidentiary certificates under both the ASIO Act and the SD Act, the courts will retain the ability to test the veracity of the evidence put before it should there be founded grounds to challenge the evidence.

Circumstances where evidentiary certificates intended to be issued

These certificates will cover circumstances where it would be difficult to prove the methods of data collection before a court without exposing sensitive law enforcement capabilities. Methods used to conceal that a computer access warrant has been executed or the methods used to covertly access a computer may be covered by an evidentiary certificate. In a criminal trial, where it may be necessary to establish the provenance of evidence called

against a defendant, it may be necessary to rely on an evidentiary certificate to prove that evidence was collected as a result of a CAW.

These certificates will relate to technical questions and not substantial matters of fact or questions of law, consistent with existing Commonwealth policy. For example, it may be that a certain vulnerability within a device was utilised to execute a CAW. Enquiries into these actions may put at risk existing operations also utilising that vulnerability, or cause that vulnerability be ineffective due to criminals avoiding applications with that vulnerability. The Government views that evidentiary certificates to protect capabilities and methodology is critical to maintaining law enforcement's ability to effectively utilise Commonwealth surveillance device laws.

Impact of issuing evidentiary certificates on individual rights

The Government recognises that the Bill engages the certain rights, such as Article 14(2) of the ICCPR. Article 14(2) provides that everyone charged with a criminal offence should have the right to be presumed innocent until proved guilty according to law. However, such a limitation will be permissible when it is reasonable in the circumstances.

Amendments to the evidentiary certificate provisions within the ASIO Act and the new evidentiary certificate provisions within the SD Act create a presumption as to the existence of the factual basis on which the certificate is issued which requires the defendant to disprove the matters certificate in the evidentiary certificate if they seek to challenge them. However, under these proposed amendments, these matters will only be details of sensitive information such as how the evidence was obtained and by whom, or that acts undertaken by service providers were likely to assist ASIO in the performance of its functions in relation to a CAW. These are necessary to achieve the legitimate objective of protecting both ASIO's and law enforcement agencies' sensitive operating capabilities and investigations. They will not however establish the weight or veracity of the evidence itself which is a matter for the court. Importantly, they will not extend to matters that are elements of the offence.

As noted above, the defendant will not be prevented from leading evidence to challenge a certificate issued under the proposed amendments. The nature of a prima facie evidence certificate regime provides an ability for the accused to seek to establish illegality – that is, to seek to establish that acts taken in order to give effect to a warrant contravened the ASIO Act or the SD Act should they choose to do so within the boundaries of the judicial framework, an put the party bringing the proceedings to further proof. However, regardless of the evidentiary certificate regime, the prosecution will still have to make out all elements of any offence.

1.139 The committee therefore seeks the minister's detailed justification for setting a penalty of five to 10 years imprisonment for a failure to comply with an assistance order, by reference to comparable Commonwealth offences.

Justification for raising penalties for non-compliance with assistance orders

The increased penalties for non-compliance with an assistance order brings this offence into line with the penalties for the types of offences that may be investigated under an assistance order. The increased penalty for non-compliance with an assistance order in the Crimes Act is appropriate to incentivise compliance with law enforcement investigations into offences

with penalties of two years or less. The higher available penalty for non-compliance with the assistance order makes cooperation with law enforcement a rational outcome.

The aggravated offence of non-compliance with an assistance order, an offence that carries a penalty of ten years, may be appropriate when investigating an individual for terrorism offences or serious offences of two years or more. For instance, some terrorism offences under the *Criminal Code Act 1995* carry a sentence of life imprisonment but failure to provide access to a device which may contain evidence of that offence would currently attract a penalty of a maximum of two years imprisonment. In these instances the incentive to assist is significantly diminished. Thus the current penalty is not commensurate with the seriousness of the span of offences which lead law enforcement to request the assistance order.

1.140 The committee also seeks the minister's advice as to whether it is intended that the offence of a failure to comply with an assistance order would abrogate the common law privilege against self-incrimination (and if not, why the explanatory memorandum suggest the higher penalty is to incentivise a suspect to comply with the order).

Intention of offence of non-compliance with an assistance order with regards to the common law privilege against self-incrimination

The offence of failure to comply with an assistance order does not currently, and will not under the proposed legislation, abrogate the common law right to freedom from self-incrimination. Assistance orders do not engage the right because they do not compel individuals to provide evidence against their legal interest. Assistance orders only compel individuals to provide access to computers or devices in the same manner as a search warrant compels individuals to provide access to a premises.

The reference to a higher penalty being necessary to incentivise compliance in the Explanatory Memorandum addresses the situation under the current penalties where individuals may opt for a lighter penalty by refusing to comply with an assistance order to conceal evidence of a serious crime. The current maximum penalty of two years imprisonment in the Crimes Act, and six months in the *Customs Act 1901* (Customs Act), is insufficient where the individual may be concealing evidence of a crime with a higher maximum penalty. In order to close this loophole, a Judge must have the ability to match the penalty for non-compliance with an assistance order to the penalty of the underlying offence being investigated.

1.146 The committee requests the minister's advice as to why it is considered necessary and appropriate to confer immunity from civil liability in item 119A of Schedule 2 and item 2 of Schedule 5, such that affected persons would no longer have a right to bring an action to enforce their legal rights.

Necessity and appropriateness of conferring immunity from civil liability with regards to item 119A of Schedule 2 and item 2 of Schedule 5

The provisions identified by the Committee will grant immunity from civil liability for things done while testing interception capabilities. The second identified provision will grant civil

immunity to individuals who provide voluntary assistance to ASIO or offer unsolicited assistance in good faith.

As in the case of the civil immunity provisions in Schedule 1, providers and individuals who provide assistance to law enforcement to test an interception capability or provide ASIO with information should not be at risk of accruing civil liability as a result. The Government considers the possibility of civil action would disincentivise compliance with authorisations to test interception capabilities and ASIO's power to request assistance. Additionally, the risk of civil liability may prevent individuals from voluntarily furnishing ASIO with information.

These provisions are likely to engage and limit the common law right to bring an action to enforce legal rights where the acts of the individual or provider would ordinarily make them civilly liable. However, this limitation is necessary to create an environment hospitable to individuals willing to cooperate with interception agencies and ASIO to promote the national interest.

The new civil immunity powers created under Schedule 2 are limited by the existing purposes for which a duty may be imposed on a provider in the subsections of section 313 of the Telecommunications Act. The relevant purposes include enforcing the criminal law and safeguarding national security. In the case of the provisions of Schedule 5 relating to ASIO informants, the immunity is not available to activities which involve committing offences against the laws of the Commonwealth, a state or a territory, or conduct that results in significant loss or damage to property. These are significant limitations which will confine the scope of civil claims which can be defeated by the immunity.

Furthermore, both the immunities granted by Schedule 2 and Schedule 5 are consistent with the circumstances in which civil immunity may be granted under subsection 313(5) of the Telecommunications Act which includes immunity for compliance with a direction and compliance in good faith with a direction.

The Hon Darren Chester MP

Minister for Veterans' Affairs
Minister for Defence Personnel
Minister Assisting the Prime Minister for the Centenary of ANZAC

MS18-000867

04 NOV 2018

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator Helen

Thank you for your letter of 18 October 2018 requesting further information on the Veterans' Affairs Legislation Amendment (Omnibus) Bill 2018.

I have attached my response to the Senate Standing Committee for the Scrutiny of Bills' Digest 12 of 2018, as requested in your correspondence.

Yours sincerely

DARREN CHESTER
Encl

Parliament House
CANBERRA ACT 2600

Telephone: 02 6277 7820
Email: minister@dva.gov.au

Veterans' Affairs Legislation Amendment (Omnibus) Bill 2018

The Veterans' Affairs Legislation Amendment (Omnibus) Bill 2018 (the Bill) received Royal Assent on 25 October 2018 and commenced on 26 October 2018. Schedule 2 amends the *Safety, Rehabilitation and Compensation (Defence-related Claims) Act 1988* (DRCA) to insert a new legal framework to enable the Military Rehabilitation and Compensation Commission (MRCC) to be provided information and/or documents relevant to the determination of defence related injuries and deaths. This legal framework inserted into the DRCA is modelled on the existing framework within the *Military Rehabilitation and Compensation Act 2004* at section 406.

In *Scrutiny Digest 12 of 2018*, the Standing Committee for the Scrutiny of Bills requested more detailed advice as to why it is considered necessary and appropriate to:

- confer on the Military Rehabilitation and Compensation Commission broad powers to require information and documents from 'any person', and to require 'any person' to appear before the Commission to give evidence;
- apply strict liability to the offence in proposed subsection 151(9); and
- include an offence-specific defence (which reverses the evidential burden of proof) in proposed subsection 151(11).

Response

Subsection 151(1) provides that the MRCC may give written notice to any person requiring the person, for the purposes of this Act, (a) to provide the MRCC (or a specified staff member assisting the MRCC) such information as the MRCC requires, or (b) produce to the MRCC any documents in the custody or under the control of a person, or (c) to appear before a specified staff member assisting the MRCC to answer questions.

Subsection 151(9) imposes an offence of strict liability where the person fails to comply with a notice under subsection (1), punishable by a penalty of 10 penalty units. Subsection 151(10) provides that an offence against subsection (9) is an offence of strict liability.

Subsection 151(11) provides that subsection (9) does not apply to the extent that the person is not capable of complying with the notice.

Coercive powers – subsection 151(1), to require information/documents from 'any person'

The decision to use the phrase 'any person' was taken during the drafting process to ensure the provision does not inadvertently limit the persons to whom the MRCC may issue a written notice to provide information and/or documents or require their appearance to answer questions.

'Any person' may be inclusive of executive officers of the Commonwealth and third parties in positions of responsibility, such as financial institutions, previous employers, accountants and medical professionals. The use of 'any person' is inclusive of all classes of people who may have custody, or be in the care or control of, the required information or document critical to a person's claim that is before the MRCC for determination. This broad

inclusionary provision is required to encompass all persons whom the MRCC and claimant reasonably believe may have custody or be in the care or control of the required information and/or document.

The information and/or document required by the MRCC is critical to the determination of a claim made in relation to a defence related injury or death (liability and/or financial compensation), including determinations necessary to effect payments to veterans and their families. This provision assists in the administration of the Department of Veterans' Affairs legislation and assists the MRCC in providing fair outcomes in relation to a claim for a defence related injury or death.

Strict liability and reversal of evidential burden of proof – subsections 151(9) and (11)

The information and/or document required by the MRCC under subsection 151(1) of the DRCA may include employment records, records made and maintained by medical providers and bank account records held by financial institutions. In many cases, the person has a legal obligation to maintain records for a specific period or the information is retained in perpetuity. However, the information/document may be inaccessible or access may incur significant costs to the claimant, which is avoided by the MRCC going directly to the holder of the records (as is the case for historical statements held by financial intuitions who charge a fee to provide statements). In the case where the claimant is vulnerable or another person is legally entitled to make a claim (a spouse or partner of a deceased Australian Defence Force member), they may experience significant barriers to providing information and/or documents to support the claim to the MRCC such as financial cost of access. There is little that can be done by the Department to otherwise incentivise these third parties to provide this information.

The Committee has requested advice as to why Schedule 2 of the Bill imposes an offence-specific defence in subsection 151(11). The Committee is concerned that this provision reverses the evidential burden of proof and asks for a response that explicitly address the relevant principles of the *Guide to Framing Commonwealth Offences* (the Guide).

The offence-specific defence allows the person issued with the notice to raise evidence that they are not capable of complying with the request in the notice. This could include that they are not the person with custody of the required information/document nor are they the person in the care and control of it. The existence of a reason not to provide the information and/or document would be a matter peculiarly within the knowledge of the person issued the notice and it would be significantly more difficult and costly for the MRCC to disprove this than the person issued the notice to establish. These factors satisfy the principles in the Guide applicable to offence-specific defences[1].

The imposition of an offence-specific defence would not lead to an unjust outcome. This is because it is reasonable in the circumstances that the person issued the notice under

---

[1] Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers,* September 2011, p. 50.

subsection 151(11) is believed to be the last known person with custody or has the care and control of the document/information required by the MRCC. This is a reason why this has been cast as a defence. Generally, the person issued the notice would have access to the information/document and their compliance with the notice would not incur any cost, or the cost would not be significant.

The appropriate burden of proof applies to offence-specific defence in subsection 151(11). The principle in the Guide is that an evidential burden should generally apply to offence-specific defences[2].

[2] Attorney-General's Department, *A Guide to Framing Commonwealth Offences. Infringement Notices and Enforcement Powers,* September 2011, p. 51 .