The Senate

Standing Committee for the Scrutiny of Bills

Scrutiny Digest 14 of 2018

28 November 2018

ISSN 2207-2004 (print)
ISSN 2207-2012 (online)

This document was prepared by the Senate Standing Committee for the Scrutiny of Bills and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Membership of the Committee

Current members

Senator Helen Polley (Chair)	ALP, Tasmania
Senator John Williams (Deputy Chair)	NATS, New South Wales
Senator Jonathon Duniam	LP, Tasmania
Senator Jane Hume	LP, Victoria
Senator Janet Rice	AG, Victoria
Senator Murray Watt	ALP, Queensland

Secretariat

Ms Anita Coles, Secretary

Mr Michael Sloane, Principal Research Officer

Mr Andrew McIntyre, Senior Research Officer

Ms Ingrid Zappe, Legislative Research Officer

Committee legal adviser

Associate Professor Leighton McDonald

Committee contacts

PO Box 6100
Parliament House
Canberra ACT 2600

Phone: 02 6277 3050

Email: scrutiny.sen@aph.gov.au

Website: http://www.aph.gov.au/senate_scrutiny

TABLE OF CONTENTS

Introduction

Terms of reference

Since 1981 the Senate Standing Committee for the Scrutiny of Bills has scrutinised all bills against certain accountability standards to assist the Parliament in undertaking its legislative function. These standards focus on the effect of proposed legislation on individual rights, liberties and obligations, and on parliamentary scrutiny. The scope of the committee's scrutiny function is formally defined by Senate standing order 24, which requires the committee to scrutinise each bill introduced into the Parliament as to whether the bills, by express words or otherwise:

(i) trespass unduly on personal rights and liberties;

(ii) make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers;

(iii) make rights, liberties or obligations unduly dependent upon non-reviewable decisions;

(iv) inappropriately delegate legislative powers; or

(v) insufficiently subject the exercise of legislative power to parliamentary scrutiny.

Nature of the committee's scrutiny

The committee's long-standing approach is that it operates on a non-partisan and consensual basis to consider whether a bill complies with the five scrutiny principles. In cases where the committee has scrutiny concerns in relation to a bill the committee will correspond with the responsible minister or sponsor seeking further explanation or clarification of the matter. If the committee has not completed its inquiry due to the failure of a minister to respond to the committee's concerns, Senate standing order 24 enables Senators to ask the responsible minister why the committee has not received a response.

While the committee provides its views on a bill's level of compliance with the principles outlined in standing order 24 it is, of course, ultimately a matter for the Senate itself to decide whether a bill should be passed or amended.

Publications

It is the committee's usual practice to table a *Scrutiny Digest* each sitting week of the Senate. The Digest contains the committee's scrutiny comments in relation to bills introduced in the previous sitting week as well as commentary on amendments to bills and certain explanatory material. The Digest also contains responses received in relation to matters that the committee has previously considered, as well as the committee's comments on these responses. The Digest is generally tabled in the Senate on the Wednesday afternoon of each sitting week and is available online after tabling.

General information

Any Senator who wishes to draw matters to the attention of the committee under its terms of reference is invited to do so. The committee also forwards any comments it has made on a bill to any relevant Senate legislation committee for information.

Chapter 1

Bills with no committee comment

1.1 The committee has no comment in relation to the following bills which were introduced into the Parliament between 12 – 15 November 2018:

- Australian Research Council Amendment (Ensuring Research Independence) Bill 2018;
- Fair Work Amendment (Restoring Penalty Rates) Bill 2018 [No. 2]; and
- Parliamentary Joint Committee on the Australia Fund Bill 2018.

Commentary on amendments and explanatory materials

Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017
[Digests 1 & 3/18]

1.2 On 15 November 2018 the Senate agreed to 222 Government amendments, the Minister for Finance and the Public Service (Senator Cormann) tabled a supplementary explanatory memorandum and the bill was read a third time.

1.3 In *Scrutiny Digest 1 of 2018 and Scrutiny Digest 3 of 2018*, the committee raised concerns that proposed section 287AA would appear to allow the minister, by legislative instrument, to determine that certain classes of Australian residents are not 'allowable donors'. The committee noted that this is a significant element of the electoral reforms proposed by the bill, is central to a number of proposed offences and civil penalty provisions and should be included in primary, rather than delegated, legislation. The committee also raised concerns that the bill did not include any specific consultation obligations in relation to instruments made under proposed section 287AA. Amendment 23 omits section 287AA, and replaces it with a new section defining 'foreign donor', which does not include a power to determine significant matters by legislative instrument. This would appear to address the committee's concerns in relation to this matter.

1.4 In *Scrutiny Digest 1 of 2018* and *Scrutiny Digest 3 of 2018*, the committee raised concerns that proposed sections 302E to 302L would create a number of offences relating to the giving and receiving of gifts, punishable by significant custodial penalties (between 5 and 10 years' imprisonment). Amendments 106 to 126 would (among other matters) replace the custodial penalties in proposed sections 302E to 302J with pecuniary penalties, and increase financial thresholds for the offences. This would appear to address the majority of the committee's concerns in relation to this matter.

1.5 The committee also notes that amendments 115 and 120 would (among other matters) introduce new offence-specific defences in relation to the offences in proposed sections 302D and 302E, which reverse the evidential burden of proof. The committee notes that no justification for reversing the evidential burden of proof is included in the supplementary explanatory memorandum.

1.6 The committee welcomes amendment 23, which replaces the definition of 'allowable donor' in proposed section 287AA with a definition of 'foreign donor'. The committee notes that the definition of 'foreign donor' does *not* include a power for the minister to determine significant matters by delegated legislation.

1.7 The committee welcomes amendments 106 to 126, which replace the significant custodial penalties for the offences in proposed sections 302D to 302L with pecuniary penalties, and increase applicable financial thresholds.

1.8 In relation to amendments 115 and 120, the committee considers that it would be appropriate for information regarding why it is considered necessary and appropriate to reverse the evidential burden of proof to be included in the explanatory memorandum.

My Health Records Amendment (Strengthening Privacy) Bill 2018
[Digests 10/18]

1.9 On 14 November 2018 the Senate agreed to two Pauline Hanson's One Nation amendments. On 15 November 2018 the Senate agreed to eight Government and one Australian Greens amendments, the Minister for Indigenous Affairs (Senator Scullion) tabled a supplementary explanatory memorandum and the bill was read a third time.

1.10 Government amendment 6 inserts proposed sections 70A, 71A and 71B into the bill. Proposed paragraph 70A(1)(b) would provide that information in a healthcare recipient's My Health Record is used for a 'prohibited purpose' if the information is used for a purpose prescribed by the regulations. Proposed sections 71A and 71B seek to impose criminal and civil penalties for using information derived from the My Health Records system for a prohibited purpose.[1]

1.11 From a scrutiny perspective, it is desirable for the content of an offence or civil penalty provision to be clear from the provision itself, so that the scope and effect of the offence or civil penalty provision is clear and so that affected persons may readily ascertain their obligations. In this instance, it appears that persons may be required to consult the regulations to determine whether an offence or civil penalty provision applies to their conduct (that is, whether they have used health information for a 'prohibited purpose').

1.12 Government amendment 8 would provide for a number of matters relating to the Data Governance Board (the Board). Proposed subsection 96G(1) seeks to provide that the Board may, with consent from the secretary, delegate any or all of its functions to any APS employee. Proposed subsection 96G(2) seeks to provide that the Board may, with consent from the data custodian,[2] delegate any or all of its

---

1 The offence would be punishable by 5 years' imprisonment, 300 penalty units, or both. A contravention of the civil penalty provision would be punishable by 1,500 penalty units.

2 Government amendment 8 also seeks to define 'data custodian' as the Australian Institute of Health and Welfare.

functions to any staff member of the Australian Institute of Health and Welfare (AIHW). The supplementary explanatory memorandum states that:

> There may be circumstances where it is appropriate for the Board to delegate a function to an employee of the Department of Health or the data custodian (i.e. the Australian Institute of Health and Welfare). New section 96G will enable the Board to do so, with permission from the respective head of the agency. To ensure effective delegation to the appropriate person, it is important that there is the ability to delegate to APS staff at all levels.[3]

1.13 While noting this explanation, the committee is concerned that proposed section 96G would permit the Board to delegate its functions and powers (which appear to include significant powers relating to the protection of health data) to *any* APS employee or *any* staff member of the AIHW. The committee notes in this regard that the bill does not appear to set limits on the level to which functions and powers may be delegated, nor impose requirements that delegates possess qualifications or expertise appropriate to the relevant delegation. The committee also notes that it does not consider the explanation in the supplementary explanatory memorandum to be sufficient to justify the breadth of the delegation in proposed section 96G.

1.14 The committee draws its scrutiny concerns in relation to government amendments 6 and 8 to the attention of senators, and leaves to the Senate as a whole the appropriateness of:

- **leaving a significant element of the offences and civil penalty provisions in proposed sections 71A and 71B to regulations; and**
- **allowing the Data Governance Board to delegate its functions and powers to *any* level APS employee, or to *any* staff member of the Australian Institute of Health and Welfare.**

3 Supplementary explanatory memorandum, p. 19.

Chapter 2

Commentary on ministerial responses

2.1 This chapter considers the responses of ministers to matters previously raised by the committee.

Agricultural and Veterinary Chemicals Legislation Amendment (Streamlining Regulation) Bill 2018

Purpose	This bill seeks to amend various Acts relating to agricultural and veterinary chemicals to: • enable the use of new, simpler regulatory processes for low-risk chemical products; • provide the Australian Pesticides and Veterinary Medicines Authority (APVMA) and industry with more flexibility to deal with certain types of new information provided when the APVMA is considering an application; • provide extensions to limitation periods and protection periods; • support computerised decision-making by the APVMA; • provide for a legislative instrument made by the APVMA to prescribe a scheme that would allow applicants and the APVMA to use accredited third party providers to undertake assessment services; • improve the transparency of voluntary recalls; • harmonise the need to inform the APVMA of new information relating to safety criteria so that the same obligations apply to all holders and applicants; • amend the procedure when dealing with minor variations in the constituents in a product; • provide the APVMA with more options when dealing with false or misleading information, and clarify what information must be included on a label; • allow the holder of a suspended product to address the reason for the suspension; • correct anomalies in the regulation-making powers for the labelling criteria; • amend APVMA's corporate reporting requirements.

Portfolio	Agriculture and Water Resources
Introduced	House of Representatives on 18 October 2018
Bill status	Before the House of Representatives

Significant matters in delegated legislation[1]

2.2 In *Scrutiny Digest 13 of 2018*[2] the committee requested the minister's detailed advice as to:

- why it is considered necessary and appropriate to leave all of the content of the proposed accreditation scheme to delegated legislation;
- the appropriateness of amending the bill so as to include at least high-level guidance as to the requirements of the proposed accreditation scheme; and
- 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).

Minister's response[3]

2.3 The minister advised:

> *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

1 Schedule 1, item 43, proposed section 6G. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(iv) and (v).

2 Senate Scrutiny of Bills Committee, *Scrutiny Digest 13 of 2018*, at pp. 1-4.

3 The minister responded to the committee's comments in a letter 27 November 2018. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 14 of 2018* available at: www.aph.gov.au/senate_scrutiny_digest

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.

Committee comment

2.4 The committee thanks the minister for this response. The committee notes the minister's advice that the proposed accreditation scheme will continue the current practice whereby it is 'entirely within the APVMA's remit' to develop and amend technical requirements for scientific assessment and that the APVMA will remain, in all cases, the decision maker under the agricultural and veterinary chemicals legislation. The committee also notes the minister's advice that the proposed scheme will provide flexibility in how the APVMA obtains an assessment of an applicant's data, including the use of third-party assessments, and that the APVMA is best placed to determine the requirements for any third-party accreditation scheme.

2.5 The committee also notes the minister's advice that the persons who could become accredited assessors would be 'constrained to those with particular expertise and knowledge necessary for conducting assessments for the approval of agvet chemicals', and that adjustments to the scheme may also be necessary to adapt to scientific and methodological changes and to improve the scheme, a process that may be hampered if the 'detailed content' of the scheme is placed in primary legislation. The committee further notes the minister's advice that it is not considered appropriate or necessary to include legislative guidance beyond that contained in proposed subsection 6G(2).

2.6 Finally, the committee notes the minister's advice that including specific consultation requirements in the bill in relation to the proposed accreditation

scheme would 'misalign' with the existing consultation requirements within the APVMA's legislative instrument making framework, and 'may limit the APVMA's ability to respond to urgent situations.'

2.7 However, the committee reiterates its view that significant matters, such as a scheme to accredit persons to perform functions in relation to the Agricultural and Veterinary Chemicals Code, should be included in primary legislation unless a sound justification for the use of delegated legislation is provided. The committee does not consider that the need for administrative flexibility adequately justifies leaving the entirety of the content of the scheme to delegated legislation.

2.8 While the committee notes the minister's advice that it would not be appropriate to include the detailed content of the scheme in primary legislation, it remains unclear why at least high-level guidance as to the requirements of the scheme could not be included in the bill. For instance, it is not clear why it would not be appropriate to amend the bill to constrain those who may become accredited assessors to persons with the particular expertise and knowledge necessary for conducting assessments for the approval of agricultural and veterinary chemicals, as the minister advises will be the case in any event.

2.9 The committee also reiterates its view that it would be appropriate to include specific consultation requirements (beyond those in section 17 of the *Legislation Act 2003*) in the bill in relation to the legislative instrument that will set out the accreditation scheme, and that compliance with these obligations be made a condition of the validity of the legislative instrument. The committee does not consider that a 'misalignment' with the APVMA's existing consultation obligations in relation to other legislative instruments provides a sufficient reason not to include such a consultation obligation in this case. The committee notes that it would be possible to include provisions allowing such additional consultation obligations to be overridden in urgent circumstances that threaten to compromise the agricultural and veterinary chemicals regulation framework.

2.10 The committee considers that it may be appropriate for the bill to be amended to include at least high-level guidance as to the requirements of the proposed accreditation scheme.

2.11 The committee considers that it would be appropriate for the bill to be amended to include specific consultation obligations (beyond those in section 17 of the *Legislation Act 2003*) in relation to the legislative instrument that will set out the proposed accreditation scheme, with compliance with such obligations a condition of the validity of the legislative instrument.

2.12 The committee otherwise draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness allowing all of the content of a scheme to accredit persons to perform functions in relation to the Agricultural and Veterinary Chemicals Code (noting that contraventions of the requirements under the scheme may be subject to penalties prescribed in the regulations) to delegated legislation.

Copyright Amendment (Online Infringement) Bill 2018

Purpose	This bill seeks to amend the *Copyright Act 1968* to: • allow injunctions to be made in respect of an online location that has 'the primary purpose or the *primary effect*' of infringing, or facilitating an infringement of copyright; • introduce a rebuttable evidentiary presumption that an online location is outside Australia; • enable the courts to order that an online search engine provider take reasonable steps so as not to provide search results that refer users to blocked online locations; • clarify the injunctive powers of the Federal Court relating to copyright; and • enable the minister to make a legislative instrument declaring that certain online search engine providers be exempted from the scheme.
Portfolio	Communications and the Arts
Introduced	House of Representatives on 18 October 2018
Bill status	Before the Senate

Significant matters in delegated legislation[4]

2.13 In *Scrutiny Digest 13 of 2018*[5] the committee requested the minister's advice as to why it is necessary to enable delegated legislation to be made to exempt certain online search engine providers from the copyright injunctive scheme, and the appropriateness of instead amending the bill so as to specifically exclude certain classes of smaller providers.

Minister's response[6]

2.14 The minister advised:

> Specifically, the Committee has sought advice on the operation of item 9 of the Bill, which would introduce new subsection 115A(8B) to the

4 Schedule 1, item 9, proposed subsection 115A(8B). The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(iv) and (v).

5 Senate Scrutiny of Bills Committee, *Scrutiny Digest 13 of 2018*, at pp. 6-7.

6 The minister responded to the committee's comments in a letter dated 22 November 2018. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 14 of 2018* available at: www.aph.gov.au/senate_scrutiny_digest

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.

Committee comment

2.15 The committee thanks the minister for this response. The committee notes the minister's advice that the search engine market is rapidly developing and that significant advancements have occurred since the website blocking scheme commenced in 2015. The committee also notes the advice that search functionality is built in to 'virtually all websites and apps' to varying degrees, and that it is not possible to foresee the nature of future developments in the types and range of search engine services. The committee also notes the minister's advice that search engine providers are not specifically defined in other Australian statutes, and that the 'vast majority' of international jurisdictions also do not possess such a statutory definition.

2.16 The committee further notes the advice that amending the bill to specifically exclude certain classes of small providers would risk failing to accurately identify intended parties, given the rapid changes mentioned above. The committee also notes the advice that the proposed approach provides the minister with a more flexible way of dealing with the potential that an injunction may be brought against a party to which the injunctive scheme is not intended to apply, and that the cost and time associated with a Federal Court case mean that it is not in the interests of copyright holders to pursue small providers, and that this has not occurred with the injunctions that have been sought against carriage service providers to date. Finally, the committee notes the advice that subsection 115A(5) of the *Copyright Act 1968* sets out a range of factors the Court may take into account when deciding whether to grant an injunction, and that this 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.'

2.17 While the committee appreciates that it may be impractical to specifically exclude certain classes of smaller providers in primary legislation, it retains scrutiny concerns about the breadth of the minister's proposed 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, or an application to vary an injunction. The committee reiterates that the bill, as it is currently drafted, would enable the minister to exclude *any* online search engine provider from the proposed injunctive scheme. It is not clear to the committee why it would not be appropriate to include in the bill at least high-level guidance to ensure this power is only exercised to

achieve the ends identified in the explanatory memorandum and by the minister's response—that is, to prevent an injunction being sought against smaller operators or those sites for which search functionality is peripheral to their activities.

2.18 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.19 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of enabling delegated legislation to be made to exempt *any* online search engine providers from the copyright injunctive scheme.

Higher Education Support (Charges) Bill 2018

Purpose	This bill seeks to impose an annual charge on all higher education providers whose students are entitled to HECS-HELP assistance or FEE-HELP assistance under the *Higher Education Support Act 2003*
Portfolio	Education and Training
Introduced	House of Representatives on 19 September 2018
Bill status	Before the House of Representatives

Charges in delegated legislation[7]

2.20 In *Scrutiny Digest 12 of 2018*[8] the committee requested 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.

Minister's response[9]

2.21 The minister advised:

> 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

7 Clause 7. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(iv).

8 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 6-7.

9 The minister responded to the committee's comments in a letter dated 16 November 2018. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 14 of 2018* available at: www.aph.gov.au/senate_scrutiny_digest

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.

Committee comment

2.22 The committee thanks the minister for this response. The committee notes the minister's advice that the purpose of allowing the amount of the charge to be set by legislative instrument is to ensure that the charge can be reviewed and updated annually. The committee also notes the advice that this approach is consistent with the *VET Student Loans (Charges) Act 2016*, and that the minister considers the requirement under subclause 7(2)—that the minister must be satisfied that the effect of the regulations will be to recover no more than the Commonwealth's likely costs in connection with the administration of the *Higher Education Support Act 2003* before the legislative instrument can be made—to be sufficient

2.23 However, the committee takes this opportunity to reiterate that one of the most fundamental functions of the Parliament is to levy taxation.[10] The committee's consistent scrutiny view is that it is for the Parliament, rather than makers of delegated legislation, to set a rate of tax. Therefore, where there is any possibility that a charge could be characterised as general taxation, the committee considers that guidance in relation to the level of a charge should be included on the face of the primary legislation.

2.24 The committee reiterates that the bill neither specifies a maximum charge nor contains any guidance that would limit the imposition of the charge to recovering only the Commonwealth's likely administrative costs (rather, it is limited

10 This principle has been a foundational element of our system of governance for centuries: see, for example, article 4 of the *Bill of Rights 1688*: 'That levying money for or to the use of the Crown by pretence of prerogative without grant of Parliament for longer time or in other manner than the same is or shall be granted is illegal'.

to whether the minister is satisfied of certain matters). It remains unclear to the committee why it would not be appropriate to specifically include guidance in the bill in relation to the method of calculation of a maximum charge. The committee also emphasises that its scrutiny concerns in relation to this matter are not alleviated by the fact that a similar approach has been taken in other legislation.

2.25 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of allowing delegated legislation to determine the amount of a charge without any guidance on the face of the bill as to the method of calculation or the maximum amount of the charge.

2.26 The committee also draws this matter to the attention of the Senate Standing Committee on Regulations and Ordinances for information.

Higher Education Support Amendment (Cost Recovery) Bill 2018

Purpose	This bill seeks to amend the *Higher Education Support Act 2003* (the Act) to: • implement an application fee for applications for approval as higher education providers whose students are entitled to FEE-HELP assistance under the Act; and • reflect the introduction of an annual charge on higher education providers under the Higher Education Support (Charges) Bill 2018
Portfolio	Education and Training
Introduced	House of Representatives on 19 September 2018
Bill status	Before the House of Representatives

Significant matters in delegated legislation[11]

2.27 In *Scrutiny Digest 12 of 2018*[12] the committee requested 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; and
- if it is considered appropriate to leave such matters to delegated legislation, the bill does not require that the Guidelines make review rights available.

Minister's response[13]

2.28 The minister advised:

> 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

11 Schedule 1, Part 2, item 3, proposed subsection 19-66(2). The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(iv).

12 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp.8-9.

13 The minister responded to the committee's comments in a letter dated 16 November 2018. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 14 of 2018* available at: www.aph.gov.au/senate_scrutiny_digest

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.

Committee comment

2.29 The committee thanks the minister for this response. The committee notes the minister's advice that leaving administrative issues, such as the setting of the rate of a penalty for late payment and the right of review of decisions made in relation to the collection and recovery of the annual charge and application fee, to delegated legislation 'facilitates a more timely and efficient response to administrative changes for the cost recovery charges.' The committee also notes the advice that this approach follows that taken in relation to the VET Student Loans course provider charge.

2.30 However, the committee reiterates its view that the amount of a penalty or the review of decisions relating to the collection and recovery of the higher education provider charge are significant matters that should generally be included in primary legislation unless a sound justification for the use of delegated legislation is provided. The committee does not consider that the need for administrative flexibility, nor the existence of similar provisions in other legislation, provide sufficient justification for leaving these matters to be set out in delegated legislation.

2.31 The committee welcomes the minister's undertaking to ensure that review rights in relation to the collection or recovery of higher education provider charges are included in the Higher Education Provider Guidelines (the Guidelines), despite the bill not requiring that they be included. However, given this intention to include review rights in the Guidelines in any event, it remains unclear why it would not be appropriate to include in the bill a specific requirement that the Guidelines include review rights.

2.32 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.33 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of leaving 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 to be set out in delegated legislation.

2.34 The committee also draws this matter to the attention of the Senate Standing Committee on Regulations and Ordinances for information.

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

Purpose	This bill seeks to amend various Acts in relation to telecommunications, computer access warrants and search warrants to: • introduce new provisions that will allow law enforcement and security agencies to secure assistance from key providers in the communications supply chain both within and outside Australia; and • increase agencies' ability to use a range of measures, including: - a new authority for Commonwealth, State and Territory law enforcement agencies to obtain computer access warrants; - expanding the ability of law enforcement agencies to collect evidence from electronic devices; - a new authority for the Australian Border Force to request a search warrant in respect of a person for the purposes of seizing a computer or data storage device; and - providing immunities from civil liability for cooperating with ASIO
Portfolio	Home Affairs
Introduced	House of Representatives on 20 September 2018
Bill status	Before the House of Representatives

Broad discretionary powers
Significant matters in delegated legislation
Privacy (Schedule 1)[14]

2.35 In *Scrutiny Digest 12 of 2018*[15] the committee requested the minister's 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

14 Schedule 1, item 7, various proposed sections. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i) and (ii).

15 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 12-22.

notice (insofar as the acts or things are by way of giving help to ASIO or an interception agency).[16]

Minister's response[17]

2.36 The minister advised:

> 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).[18]
>
> 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.[19] 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 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*.[20] 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

16 Schedule 1, item 7, proposed subsections 317G(6), 317L(3) and 317T(7).

17 The minister responded to the committee's comments in a letter dated 12 November 2018. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 14 of 2018* available at: www.aph.gov.au/senate_scrutiny_digest

18 Explanatory memorandum, p. 38 para 54.

19 Explanatory memorandum, pp. 45 and 47.

20 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.

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.

Operational examples from law enforcement agencies

Subsection 317(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.

Subsection 317(1)	**Listed act or thing**	**Examples**
		- 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)[21]	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 equipment, and electronic service etc.	- 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.
(f)	Assisting with the testing, modification, development or maintenance of a	- 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

21 Note, the minister's original response did not include paragraph (c).

Subsection 317(1)	**Listed act or thing**	**Examples**
	technology or capability.	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 a 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 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	- 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.

Subsection 317(1)	Listed act or thing	Examples
	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	

Operational examples from intelligence agencies

Subsection 317(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 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 account, limiting ASIO's ability to establish contemporary coverage of the group. On seeking appropriate warrants authorising ASIO 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

Subsection 317(1)	**Listed act or thing**	**Examples**
		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 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

Subsection 317(1)	**Listed act or thing**	**Examples**
		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 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

Subsection 317(1)	Listed act or thing	Examples
(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.	ongoing covert nature of ASIO's operation.
(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 a foreign country; or - the interests of Australia's national security, the interests of Australis's foreign relations or the interests of Australia's national economic well-being.	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.

Committee comment

2.37 The committee thanks the minister for this response. The committee notes the minister's advice that the acts or things that may be specified in a technical capability notice are exhaustively set out under proposed paragraphs 317E(b)-(j); however, the range of acts and things may be expanded by legislative instrument. The committee also notes the advice that the central reason for not exhaustively

setting out the acts or things that may be specified under technical assistance requests and technical assistance notices is the need to allow for 'operational flexibility in complex, technologically diverse, circumstances', and that there may be many technical things that a provider may be able to do to appropriately assist law enforcement beyond the list of activities in proposed section 317E—for example, disruption of a service being used for criminal activity. The committee also notes the advice that any additional specified assistance must be of 'the same kind, class or nature' as those acts or things listed under proposed paragraphs 317E(1)(a) to (j), connected to the eligible activities of the provider and related to the relevant agency's functions.

2.38 The committee also notes the advice that the non-exhaustive definition of listed acts or things that may be specified under technical assistance requests 'reflects the voluntary nature' of these requests and that providers are thereby protected from being required to provide kinds of assistance with which they take issue. The committee also notes the advice that the acts or things a provider may be required to do under a technical assistance notice are limited to acts or things the provider is already capable of doing, but that the bill deliberately allows a technical assistance notice to require a provider to do acts or things that fall 'beyond the precise words of the listed acts or things defined in section 317E' where they are capable of doing so, and that this is warranted because the relevant objectives in relation to which such a notice may be issued are 'sufficiently serious'.

2.39 However, the committee emphasises that its scrutiny concerns in relation to the non-exhaustive definition of acts or things that may be specified in technical assistance requests or notices stem from the broad discretion these provisions would grant to decision makers to specify acts or things, in relation to which providers would be granted civil immunity (see paragraphs 2.80 to 2.86 below). Neither the fact that a provider may refuse to cooperate with a technical assistance request, nor the fact that a company may only be required to do something which it is already capable of doing under a technical assistance notice, address this concern.

2.40 The committee also emphasises that, although both the minister's advice and the explanatory memorandum[22] state that any additional specified acts or things must be of 'the same kind, class or nature' as those listed under proposed section 317E, the bill itself does not appear to contain such a limitation. As such, the range of acts or things that may be specified in a technical assistance request or notice appear to be limited only by the requirement that they must be in connection with the eligible activities of the provider and be by way of giving help to, or be directed at a provider being capable of giving help to, the relevant agency in relation to the performance of a function or the exercise of a power insofar as it relates to a relevant objective. However, the committee also holds concerns about the breadth

22 Explanatory memorandum, pp. 45, 47.

of the relevant objectives set out in the bill (see paragraphs 2.50 to 2.58 below), and as such it is not clear that it is appropriate to allow decision makers a very broad discretion with respect to the acts or things they may specify in a technical assistance request or notice. Finally, with respect to the example of an additional act or thing the bill would allow to be specified in a technical assistance notice or request—that is, disruption of a service being used for criminal activity—it is not clear to the committee why it would not be appropriate to explicitly include such an 'often-used and necessary' function in proposed section 317E.

2.41 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.42 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of allowing '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).

Broad discretionary powers
Significant matters in delegated legislation
Privacy (Schedule 1)[23]

2.43 In *Scrutiny Digest 12 of 2018*[24] the committee requested the minister's advice as to 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).[25]

Minister's response

2.44 The minister advised:

> The Minister under subsection 317T(5) has the power to expand the definition of 'listed help' by legislative instrument. Legislative instruments

---

23 Schedule 1, item 7, various proposed sections. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i) and (ii).

24 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 12-22.

25 Schedule 1, item 7, proposed subsection 317T(5).

> 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.

Committee comment

2.45 The committee notes the minister's advice that it is considered appropriate to provide that the definition of 'listed help' may be expanded by legislative instrument as this would allow the acts or things that may be specified under a technical capability notice to be 'readily and quickly adapted' to take account of technological advances in the communications industry. The committee also notes the advice that under proposed paragraph 317T(6)(d), the minister is required to consider, among other matters, the likely impact of the determination on providers and that, while the bill would not require the minister to consult with providers prior to making a legislative instrument, such consultation would be a 'necessary step' for the minister to have due regard to this matter.

2.46 In light of the minister's advice that consultation with providers prior to making a legislative instrument would be a 'necessary step' for the minister , it is not clear to the committee why it would not be appropriate to include specific consultation obligations (beyond those in section 17 of the *Legislation Act 2003*) could not 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).

2.47 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.48 The committee considers that it would be appropriate for the bill to be amended to include specific consultation obligations (beyond those in section 17 of

the *Legislation Act 2003*) in the bill in relation to a determination made under proposed subsection 317T(5) to expand the range of acts or things that may be specified in a technical capability notice (with compliance with such obligations a condition of the validity of the legislative instrument).

2.49 The committee also draws this matter to the attention of the Senate Standing Committee on Regulations and Ordinances for information.

Broad discretionary powers
Significant matters in delegated legislation
Privacy (Schedule 1)[26]

2.50 In *Scrutiny Digest 12 of 2018*[27] the committee requested the minister's advice as to 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 offences or breaches of the law.[28]

Minister's response

2.51 The minister advised:

> 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

---

26 Schedule 1, item 7, various proposed sections. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i) and (ii).

27 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 12-22.

28 Schedule 1, item 7, proposed subsections 317G(5) and 317T(3), and proposed paragraph 317L(2)(c).

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.

Committee comment

2.52 The committee notes the minister's advice that, while the relevant objectives relating to enforcing the criminal law (including in a foreign country) and laws imposing pecuniary penalties, are wide enough to allow notices and requests to be used to pursue minor offences or breaches of the law, 'practical and investigative limitations will prevent such an outcome.' The committee also notes the advice that notices and requests are expected to be 'most usefully deployed' in support of interception and surveillance device warrants under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and the *Surveillance Devices Act 2004* (SD Act), and that the use of these underlying powers generally requires the

investigation of a serious criminal offence attracting three or more years imprisonment.

2.53 The committee also notes the minister's advice that it is important to align the purposes for which the proposed measures may be used with the thresholds for access to data under the *Telecommunications Act 1997* (Telecommunications Act) as the measures are designed to complement existing functions of agencies, and that the relevant objectives under the bill are narrower than the purposes for which analogous powers under the Telecommunications Act may be exercised.

2.54 The committee further notes the minister's advice that the requirement under proposed subsection 317ZK(3), that providers be compensated for the reasonable costs of compliance by the issuing agency, means that the proposed powers will be 'exercised sparingly and in light of budgetary constraints', and that fiscal responsibility measures mean that agencies will be 'highly unlikely to be able to deploy resources to target minor crimes.' Finally, the committee notes the advice that, while the enforcement of laws imposing pecuniary penalties would be a relevant objective, this is 'not intended to encompass small-scale administrative fines.'

2.55 In light of the minister's advice that it is not intended that notices and requests be used to pursue minor criminal offences or small-scale administrative fines, and that practical constraints mean this is highly unlikely to occur, the committee considers that it would be appropriate to amend the bill to include a legislative safeguard to exclude the possibility that the proposed framework may be used in relation to such minor offences and breaches of the law—for example, by including minimum pecuniary penalty and imprisonment thresholds in the definition of relevant objectives for each type of notice or request.

2.56 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.57 The committee considers that it may be appropriate for the bill to be amended to include a legislative safeguard to exclude the possibility that the proposed framework may be exercised in relation to minor offences and breaches of the law—for example, by including minimum pecuniary penalty and imprisonment thresholds in the definition of relevant objectives for each type of notice or request.

2.58 The committee otherwise draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of providing 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 offences or breaches of the law.

Broad discretionary powers
Significant matters in delegated legislation
Privacy (Schedule 1)[29]

2.59 In *Scrutiny Digest 12 of 2018*[30] the committee requested the minister's advice as to 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'.[31]

Minister's response

2.60 The minister advised:

> 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

---

29 Schedule 1, item 7, various proposed sections. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i) and (ii).

30 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 12-22.

31 Schedule 1, item 7, proposed subsection 317G(5).

> 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.

Committee comment

2.61 The committee notes the minister's advice that the wider range of relevant objectives in relation to which a technical assistance request may be issued 'reflects the voluntary nature of the requests'. The committee also notes the advice that the inclusion of the interests of Australia's foreign relations and national economic well-being reflects the functions of Australia's intelligence and security agencies and is intended to support technical assistance requests made by these agencies, rather than by interception agencies. The committee also notes the minister's advice that, where a provider does an act or thing in compliance with a request, in good faith purportedly in compliance with a request, it is appropriate that the provider not be at risk of civil liability as a result, including where the request was issued in the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

2.62 While noting this advice, the committee considers that it does not directly address its scrutiny concerns in relation to the wider range of relevant objectives in relation to which a technical assistance request may be issued. The committee considers that the 'interests of Australia's foreign relations' and 'the interests of Australia's national economic well-being' may encompass a very broad range of activities and neither the explanatory memorandum, nor the minister's response, provide any detail as to the nature of the activities that may fall under these objectives. The committee does not consider that the voluntary nature of a technical assistance request, nor the fact that these objectives align with the functions of Australia's intelligence and security agencies, provide a sufficient justification for

allowing the use of technical assistance requests in relation to such broadly defined objectives, noting that providers will be granted immunity from civil liability when complying with a request intended to pursue these objectives.

2.63 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.64 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of allowing 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 broadly defined objectives of the interests of Australia's 'foreign relations' or 'national economic well-being'.

Broad discretionary powers
Significant matters in delegated legislation
Privacy (Schedule 1)[32]

2.65 In *Scrutiny Digest 12 of 2018*[33] the committee requested the minister's advice as to the appropriateness of including in the bill a requirement that consultation with a provider be conducted prior to issuing a technical assistance notice, similar to the requirement under proposed section 317W in relation to a technical capability notice.

Minister's response[34]

2.66 The minister advised:

> 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.

---

32 Schedule 1, item 7, various proposed sections. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i) and (ii).

33 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 12-22.

34 The minister responded to the committee's comments in a letter dated 12 November 2018. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 14 of 2018* available at: www.aph.gov.au/senate_scrutiny_digest

> 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)[35] 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.

Committee comment

2.67 The committee notes the minister's advice that proposed section 317RA would require a decision maker to have regard to, among other matters, the interests of the relevant provider, the availability of other means to achieve the objectives of the notice, and the privacy and cybersecurity expectations of the Australian community before issuing a technical assistance notice, and that 'in most circumstances' it is expected that a decision-maker would need to consult with the provider to determine if the assistance requested is reasonable, proportionate, practical and technically feasible. The committee also notes the advice that the process is intended to mirror how consultations occur under section 313 of the Telecommunications Act—that is, agencies will 'typically engage early with a provider about possible requirements and the outcome on an eventual request reflects a negotiation between both parties'.

2.68 In light of the minister's advice that the bill would, in practice, require consultation with the relevant provider to take place before a technical assistance request is issued, the committee reiterates its view that it would be appropriate for the bill to be amended to include an explicit requirement that consultation with a provider be conducted prior to issuing a technical assistance notice, similar to the

35 See Explanatory memorandum pp. 48-49.

requirement under proposed section 317W in relation to a technical capability notice.

2.69 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.70 The committee considers that it would be appropriate for the bill to be amended to include an explicit requirement that consultation with a provider be conducted prior to issuing a technical assistance notice, similar to the requirement under proposed section 317W in relation to a technical capability notice (with compliance with such obligations a condition of the validity of the legislative instrument).

2.71 The committee also draws this matter to the attention of the Senate Standing Committee on Regulations and Ordinances for information.

Exclusion of judicial review (Schedule 1)[36]

2.72 In *Scrutiny Digest 12 of 2018*[37] the committee requested the minister's advice as to 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).

Minister's response

2.73 The minister advised:

> 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

36 Schedule 1, item 1. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(iii).

37 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp.22-23.

> 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.

Committee comment

2.74 The committee thanks the minister for this response. The committee notes the minister's advice that technical assistance notices may be issued in the course of an ongoing investigation and 'it is imperative that such a notice can be issued and used quickly'. The committee also notes the advice that review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) could 'adversely impact the effectiveness and outcomes of an investigation', and that decisions to issue technical capability notices are unsuitable for review under the ADJR Act because they are ministerial decisions to develop law enforcement and national security capabilities. The committee also notes the minister's advice that a decision to issue a technical assistance notice or a technical capability notice may be challenged on a number of grounds, and that in these cases the *Judiciary Act 1903*

(Judiciary Act) and the Constitution provide avenues for judicial review in the High Court, the Federal Court or State Supreme Courts, depending on the circumstances.

2.75 However, the committee notes that given that judicial review under the Judiciary Act and the Constitution would remain available in relation to decisions taken under proposed Part 15, it is unclear why it is considered appropriate to exclude such decisions from review under the ADJR Act. The minister's response does not explain what differences exist between judicial review processes under the ADJR Act and the Judiciary Act such that it is considered appropriate to exclude the former but not the latter. In light of the fact that the ADJR Act was enacted to rationalise and simplify the law of judicial review—by providing a more readily understandable and accessible avenue for review than that provided through the scheme of review entrenched in the Constitution—the committee considers that the mere fact that review under the Constitution (which is mirrored in the Judiciary Act) cannot be excluded does not itself provide a sufficient justification for the exclusion of the ADJR Act.

2.76 The committee also reiterates that although compulsory notices under the framework may be issued in relation to national security objectives, they may also be issued in relation to objectives relating to the enforcement of the criminal law (including foreign offences) and laws imposing pecuniary penalties. Therefore it does not appear that decisions made under proposed Part 15 would always involve matters relevant to national security. Similarly, although technical assistance notices may sometimes be issued in the course of an ongoing investigation and be subject to some urgency, it is not clear that all decisions under proposed Part 15 would be subject to the same urgency. Nor is it clear why, if it is considered that judicial review under the ADJR Act might hamper the use of technical assistance notices in urgent circumstances, review under the Judiciary Act would not have the same effect. The committee also notes that from its inception it was contemplated that the ADJR Act would enable the review of significant decisions made by ministers insofar as they are decisions of an administrative character made under an enactment.

2.77 In relation to decisions made under proposed Part 15 that do involve matters relevant to national security, the committee also notes that although the Administrative Review Council has expressed the view that national security considerations may be a reason for excluding ADJR Act review, it has stated that this should not be a blanket reason for an exemption and 'each national security exemption should be considered on its own merits, with regard to whether review of the decision could pose a risk to national security through the dissemination of information through judicial review proceedings.'[38] In this regard, the committee emphasises that there are means for mitigating or eliminating the risk that sensitive

38 Administrative Review Council, *Federal Judicial Review in Australia*, September 2012, p. 107.

security information may be disclosed in the course of ADJR Act proceedings which fall short of entirely excluding judicial review under the ADJR Act.

2.78 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.79 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of excluding judicial review under the *Administrative Decisions (Judicial Review) Act 1977* in relation to decisions made under proposed Part 15 (industry assistance).

Immunity from liability (Schedule 1)[39]

2.80 In *Scrutiny Digest 12 of 2018*[40] the committee requested 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).

Minister's response

2.81 The minister advised:

> 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[41], '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

---

39 Schedule 1, item 7, proposed paragraph 317G(1)(c), and proposed section 317ZJ. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

40 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp.23-24.

41 Explanatory memorandum p. 69 para 272

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.

Committee comment

2.82 The committee thanks the minister for this response. The committee notes the minister's advice that providers would not be liable to an action or other proceeding in the exceptional circumstances where elements of a technical assistance notice or technical capability notice are deemed invalid and that a provider is considered to have acted in good faith if the provider acts with honesty according to the standards of a reasonable person. The committee also notes the advice that complying with a technical assistance notice or technical capability notice, or acting in accordance with a technical assistance request, may involve the violation of intellectual property laws or contractual obligations, and that it is considered appropriate that a provider should not be at risk of accruing civil liability in these circumstances.

2.83 The committee also notes the minister's advice that where a provider is given civil immunity for an act or thing that is not expressly defined under proposed section 317E, the act or thing 'will necessarily have been one of the same kind, class or nature' as the listed acts or things. The committee also notes the advice that, the minister must have regard to the criteria set out under proposed subsection 317T(6) prior to making a legislative instrument to expand the acts or things that may be specified under a technical capability notice, and that 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.'

2.84 However, as noted above (see paragraph 2.40 above), the bill does not require that any additional specified acts or things must be of 'the same kind, class or nature' as those listed under proposed section 317E. In addition, the minister's response does not explain how this requirement would in practice constrain the matters which may be specified with more particularity than is achieved by the

general requirement that specified matters must be in connection with the eligible activities of the provider and be by way of giving help to, or be directed at a provider being capable of giving help to, the relevant agency in relation to the performance of a function or the exercise of a power relating to a relevant objective. Further, while the power of the minister to make a legislative instrument to expand the acts or things that may be specified under a technical capability notice is subject to the requirement that he or she have regard to certain matters, it is nevertheless possible to expand the range of acts or things a provider may be required to do without amending primary legislation. The committee therefore retains scrutiny concerns about granting immunity from civil liability to providers in relation to acts or things that either are not exhaustively set out in the bill, or may be expanded by delegated legislation.

2.85 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.86 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness providing 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 either not exhaustively set out in the bill or may be expanded by delegated legislation).

Reversal of evidential burden of proof (Schedule 1)[42]

2.87 In *Scrutiny Digest 12 of 2018*[43] the committee requested 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 reverses the burden of proof is assisted if it explicitly addresses relevant principles as set out in the *Guide to Framing Commonwealth Offences*.[44]

---

42 Schedule 1, item 7, proposed subsections 317ZF(3), (5) to (11) and (13). The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

43 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at p. 25.

44 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, pp. 50-52.

Minister's response

2.88 The minister advised:

> 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.
>
> 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*".[45]
>
> The unauthorised disclosure offence within Schedule 1 meets these criteria. Rather than require the Crown to prove this offence, relevant persons[46] 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.

Committee comment

2.89 The committee thanks the minister for this response. The committee notes the minister's advice that the government considers it appropriate to create offence-

45 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and enforcement provisions, p. 50.*

46 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.

specific defences to protect sensitive information where the information is in the hands of entrusted persons, such as those listed under proposed section 317ZF(1)(b), because 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 purposes.'

2.90 The committee also notes the minister's advice that the persons listed under proposed section 317ZF(1)(b) will be 'best-placed' to make out a defence, that the facts required to prove the defence will be matters 'peculiarly within the knowledge of these individuals or to which they have ready access', and that it is 'peculiarly within the ability' of the relevant individuals to rebut the allegation of unauthorised disclosure.

2.91 However, the committee emphasises that the test of when it is appropriate to reverse the evidential burden of proof, as set out in the *Guide to Framing Commonwealth Offences*,[47] states that it is only appropriate to include a matter in an offence-specific defence when:

- it is peculiarly within the knowledge of the defendant; *and*
- it would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter.[48]

2.92 The minister's advice does not address the question of whether the matters in the proposed offence-specific defences would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish. While the minister's advice does assert that the facts required to prove the matters will be either peculiarly within the knowledge of the relevant persons 'or readily accessible to them', it does not provide any information to establish that this would be the case for each of the relevant matters. The committee also notes that whether evidence 'is readily accessible' to the defendant is not the same as the evidence being peculiarly within the defendant's knowledge. It therefore remains unclear to the committee that it would be appropriate to reverse the evidential burden in relation to each of the matters set out in proposed subsections 317ZF(3), (5), (6), (7), (8), (9), (10), (11) and (13), some of which do not appear on their face to be peculiarly within the knowledge of the defendant (for example, whether the person was acting in accordance with requirements imposed by law or in connection with their official functions or duties).[49]

---

47 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, pp 50-52.

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

49 See, for example, the matters in proposed paragraphs 317ZF(3)(a), (c) and (d) and subsections 317ZF(5) to (11) and (13).

2.93 The committee notes that the unauthorised disclosure offence set out under proposed section 317ZF appears to criminalise the activities undertaken by any designated communications provider, public servant or engaged contractor when dealing with information obtained in accordance with or in relation to the proposed framework. The bill relies on the existence of defences to the offence, which provide that it is not an offence if a person discloses technical assistance request, technical assistance notice or technical capability notice information in specified circumstances. However, this would appear to leave officials acting appropriately in the course of their employment, or providers acting in accordance with their obligations under the framework, open to a criminal charge and then places the evidential burden of proof on the officer or provider to raise evidence to demonstrate that they were in fact acting in accordance with their employment or their obligations under the proposed framework. The committee is also concerned that some officials who, by reason of the sensitive national security nature of their work, may be unable to lawfully raise evidence relating to whether they were acting in the course of their duties.

2.94 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.95 The committee considers it may be appropriate for the bill to be amended to ensure that officials who have secrecy obligations (such as officials from the Inspector-General of Intelligence and Security) do not bear the evidential burden of proof in relation to the defences at proposed subsection 317ZF(3)-(11).

2.96 The committee otherwise draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of reversing the evidential burden of proof in relation to matters that do not appear to be peculiarly within the knowledge of the defendant.

Broad discretionary powers (Schedule 1)[50]

2.97 In *Scrutiny Digest 12 of 2018*[51] the committee requested the minister's advice 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; and

---

50 Schedule 1, item 7, proposed subsection 317ZK(1). The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(ii).

51 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 26-27.

- why (at least high-level) guidance as to the circumstances in which proposed section 317ZK will not apply cannot be included in the bill.

Minister's response

2.98 The minister advised:

> Circumstances in which it would not be appropriate to compensate a provider
>
> 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 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.

Committee comment

2.99 The committee thanks the minister for this response. The committee notes the minister's advice that it is envisioned that the Director-General of Security, the chief officer of an interception agency or the Attorney-General would only exercise the power to not apply the usual terms and conditions for compliance with a notice in 'limited circumstances where it is prudent to protect public money from unscrupulous providers or providers who cause damage through negligence'. The committee also notes the advice that the decision maker must be satisfied that waiving the usual processes is in the public interest and must have regard to the matters set out in proposed subsection 317ZK(2), that any notice that amounts to an acquisition on other than just terms would be invalid, and that a decision not to compensate a provider could be subject to judicial review under the Judiciary Act.

2.100 The committee also notes the minister's advice that the government considers it inappropriate to include further guidance in the bill as to the circumstances in which it would not be appropriate to compensate a provider subject to a technical assistance notice or technical capability notice, as decision makers would already be required to consider 'a broad range of circumstances to ensure that cases are considered on an individual basis'.

2.101 The committee also welcomes the minister's advice that the government may consider amending the bill to include the 'language of recklessness or wilful actions', which is currently set out only in the explanatory memorandum,[52] to provide greater guidance as to the circumstances in which it would be appropriate not to compensate a provider. The committee considers such an amendment would partially address its scrutiny concerns about the broad discretionary power that the public interest test under proposed subsection 317ZK(1) would grant decision makers. However, the committee retains scrutiny concerns about the unavailability of judicial review under the ADJR Act in relation to decisions not to compensate a provider (see paragraphs 2.72 to 2.79 above), and about whether a provider can reasonably be expected to know whether particular actions would cause a risk to law enforcement or security interests and thereby potentially lead to a decision that the provider should not be compensated, given that law enforcement and security agencies often operate covertly.

2.102 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic

52 Explanatory memorandum, p. 71.

material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.103 The committee considers it may be appropriate for the bill to be amended to include (at least high-level) guidance as to the circumstances in which proposed section 317ZK will not apply.

2.104 The committee otherwise draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of granting decision makers a broad discretion not to apply the general rule that a provider need only comply with a notice on a no profit, no loss basis.

Broad delegation of administrative power (Schedule 2)[53]

2.105 In *Scrutiny Digest 12 of 2018*[54] the committee requested 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.

Minister's response

2.106 The minister advised:

> 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.

---

53 Schedule 2, items 2 and 3. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(ii).

54 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 27-28.

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

Committee comment

2.107 The committee thanks the minister for this response. The committee notes the minister's advice that given the need to conceal activity under a computer access warrant, delegating power to someone with access may be necessary to ensure activities remain covert where ASIO no longer has access, and it is more appropriate that ASIO's delegation powers are determined by ASIO, rather than set out in legislation.

2.108 However, the committee reiterates that this power allows ASIO to delegate its authority in relation to the concealment of activities under a warrant to *any* person or *any class* of persons. The committee has consistently drawn attention to legislation that allows the delegation of administrative powers to a relatively large class of persons, with little or no specificity as to their qualifications or attributes. Generally, the committee prefers to see a limit set either on the scope of powers that might be delegated, or on the categories of people to whom those powers might be delegated, or at a minimum that the relevant authority be satisfied that the person to whom powers or functions are delegated possesses appropriate expertise.

2.109 The committee considers it may be appropriate to amend the bill to require that the Director-General of ASIO (or a senior position-holder authorised by the Director-General) be satisfied that persons performing delegated authority have the expertise appropriate to the authority delegated.

2.110 The committee otherwise draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of providing ASIO with a broad power to delegate its authority under a warrant to *any* person.

Coercive powers
Privacy (Schedules 2 to 5)[55]

2.111 In *Scrutiny Digest 12 of 2018*[56] the committee requested the minister's advice as to why the categories of persons eligible to issue computer access warrants should not be limited to persons who hold judicial office.[57]

55 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

56 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

57 See Schedule 2, item 49. See also Schedule 2, item 145.

2.112 The committee notes the minister did not respond to this aspect of the committee's request.

2.113 The committee reiterates that proposed subsection 27A(7) provides that an application for a computer access warrant may be made to an eligible judge or to a nominated member of the Administrative Appeals Tribunal (AAT). Section 13 of the SD Act provides that a nominated AAT member can include any member of the AAT, including full time and part-time senior members and general members. Part-time senior members and general members can only be nominated if they have been enrolled as a legal practitioner for at least five years. The committee reiterates that it has had a long-standing preference that the power to issue search warrants should only be conferred on judicial officers. In light of the extensive personal information that could be covertly accessed from an individual's computer or device, the committee would expect a detailed justification be given as to the appropriateness of conferring such powers on AAT members, particularly part-time senior members and general members.

2.114 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of specifying non-judicial office holders as being eligible to issue computer access warrants.[58]

Coercive powers
Privacy (Schedules 2 to 5)[59]

2.115 In *Scrutiny Digest 12 of 2018*[60] the committee requested the minister's advice as to 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.[61]

Minister's response

2.116 The minister advised:

> 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

58 See Schedule 2, item 49. See also Schedule 2, item 145.

59 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

60 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

61 See Schedule 2, items 6, 11 and 13.

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.

Committee comment

2.117 The committee thanks the minister for this response. The committee notes the minister's advice that it may be necessary to use interception capabilities in order to technically enable computer access. The committee notes the advice that these amendments are not lowering the threshold for interception as there are already general exceptions to the prohibition on interception, including incidental interception. However, the advice goes on to state that if law enforcement agencies and ASIO 'had to meet the thresholds for the existing interception regime' it may mean that a computer access warrant could not be executed or there would be significant delay, noting that the existing threshold for interception warrants are generally offences with a minimum of seven years imprisonment while the threshold for a computer access warrant will be for offences with a minimum of three years imprisonment.

2.118 The committee also notes the minister's advice that the objective of the measure is to enhance the operational effectiveness of the use of a computer access warrant, as delay, or inability, may result in either significant loss of evidence or the

continuation of serious crime, and to ensure that multiple warrants are not required to execute a computer access warrant.

2.119 The committee is of the view that the amendments to the ASIO Act to remove the need for ASIO to gain a separate interception warrant lowers the existing threshold for obtaining access (albeit limited access) to intercepted information. In light of the desire for a single warrant process, the committee reiterates its previous comment that it would be possible for the legislation to provide for a single warrant process but at a higher threshold for the grant of the warrant. The committee notes that the minister's response did not address this aspect of the committee's initial scrutiny comments. The committee also reiterates its general preference that the power to issue search warrants be conferred on judicial officers, whereas in the case of computer access warrants issued under the ASIO Act, the power is conferred on a member of the executive.

2.120 The committee reiterates that while there are restrictions proposed on the use of material intercepted during the execution of a computer access warrant,[62] the interception of communications over a telecommunications system has the potential to unduly trespass on personal rights and liberties, particularly the right to privacy.

2.121 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.122 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of lowering the threshold for ASIO to access intercepted communications and allowing law enforcement agencies to intercept communications in limited circumstances.

---

62 The proposed amendments to the TIA Act provide that such information can only be communicated, used, recorded or given as evidence if:

- it is for a purpose of doing a thing authorised by a computer access warrant;
- the information relates to the involvement of a person in activities that present a significant risk to a person's safety; or
- the information relates to the involvement of a person in activities: acting for, or on behalf of a foreign power; posing a risk to operational security; relating to the proliferation of weapons of mass destruction; or contravening a UN sanction enforcement law.

Coercive powers
Privacy (Schedules 2 to 5)[63]

2.123 In *Scrutiny Digest 12 of 2018*[64] the committee requested the minister's advice as to 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).[65]

Minister's response

2.124 The minister advised:

> 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.

---

63 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

64 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

65 See Schedule 2, items 50-76.

> 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.

Committee comment

2.125 The committee thanks the minister for this response. The committee notes the minister's advice that the use of emergency authorisations is not new, they are available in very limited circumstances, have various safeguards in place and in practice are rarely used. The committee also notes the minister's advice that the availability of emergency access powers is necessary to ensure that computer access powers can be used for the purposes of public safety and national security.

2.126 The committee reiterates that as a computer access warrant can involve significant coercive powers (for example, the ability to covertly access data held on particular computers, enter premises and use force), it is particularly concerned that such powers only be authorised under a warrant issued by a judicial officer. Allowing a law enforcement agency to authorise its own actions under an emergency authorisation has the potential to unduly trespass on the right to privacy. The committee notes that the fact that similar provisions exist currently in legislation is not a sufficient basis, in itself, to justify the inclusion of such powers in a bill currently before Parliament.

2.127 The committee also notes that the minister's response did not provide any information as to when it may be impractical to apply to a judge or nominated AAT member, noting that proposed section 27B would allow an application for a warrant to be made by telephone, fax, email or any other means of communication.

2.128 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of enabling 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 telephone, fax or email).

Coercive powers
Privacy (Schedules 2 to 5)[66]

2.129 In *Scrutiny Digest 12 of 2018*[67] the committee requested the minister's advice as to the appropriateness of retaining information obtained under an emergency authorisation that is subsequently not approved by a judge or AAT member.[68]

Minister's response

2.130 The minister advised:

> 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.

Committee comment

2.131 The committee thanks the minister for this response. The committee notes the minister's advice that where information obtained in the course of an investigation has investigative value it is paramount that that information be retained as it may be critical for valid investigations into serious crime, even if it is improperly obtained.

2.132 The committee reiterates that it considers that judicial oversight of intrusive powers is essential in ensuring that such powers are used appropriately. As set out

---

66 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

67 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

68 See Schedule 2, item 76, proposed section 35A(6).

above, an emergency authorisation allows a law enforcement agency to authorise its own coercive and covert actions. Where a judge or AAT member subsequently holds that the authorisation should not have been made, retaining evidence obtained improperly for investigative purposes has serious implications for personal rights and liberties. In particular, the committee notes that authorisations could be improperly made, in the knowledge that even if they are later not approved any information obtained could be retained as part of the investigation.

2.133 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of allowing information obtained under an invalid emergency authorisation to be retained for investigative purposes.

Coercive powers
Privacy (Schedules 2 to 5)[69]

2.134 In *Scrutiny Digest 12 of 2018*[70] the committee requested the minister's advice as to the appropriateness of enabling ASIO and law enforcement agencies to act to conceal anything 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.[71]

Minister's response

2.135 The minister advised:

> 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 *[sic]* 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*

---

69 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

70 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

71 See Schedule 2, items 7, 8, 12 and 49, proposed subsection 27E(7).

> *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.

Committee comment

2.136 The committee thanks the minister for this response. The committee notes the minister's advice as to why it is necessary to provide for concealment of activities undertaken under a computer access warrant. However, the committee notes that it was not questioning the necessity for concealing access under a warrant, its question was as to the appropriateness of enabling ASIO and law enforcement agencies to act to conceal anything done under a warrant *after* the warrant has ceased to be in force. As noted in its initial analysis, these provisions authorise the agencies to do anything reasonably necessary to conceal the fact that anything has been done under a warrant, enter premises, remove anything to conceal things, add, copy, delete or alter data and intercept communications, at any time while the warrant is in force or within 28 days after it ceases to be in force. In addition, the bill provides that if concealment activities have not been done within 28 days after the warrant ceases to be in force, those things can be done at the earliest time after that 28 day period in which it is reasonably practicable.[72]

2.137 The committee acknowledges that there may be difficulties in knowing when the process of concealment may be complete, however, there are scrutiny concerns in allowing agencies to exercise coercive powers after a warrant has ceased to be in force. The committee reiterates that it considers it would be possible to have a separate statutory process for applying for a new warrant to allow the agency to carry out concealment activities, which would remove concerns about not being able to meet the statutory threshold for obtaining a new computer access warrant, but

72 Schedule 2, item 7, proposed paragraph 25A(8)(k); item 8, proposed paragraph 27A(3C)(k); item 12, proposed paragraph 27E(6)(k); and item 49, proposed paragraph 27E(7)(k).

would ensure coercive powers are undertaken under an existing warrant. The committee notes that the minister's response did not address its question as to 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.

2.138 The committee considers it may be appropriate to amend the bill to provide a process for obtaining a separate concealment of access warrant if the original warrant has ceased to be in force.

2.139 The committee otherwise draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of enabling ASIO and law enforcement agencies to act to conceal anything done under a warrant *after* the warrant has ceased to be in force.

Coercive powers
Privacy (Schedules 2 to 5)[73]

2.140 In *Scrutiny Digest 12 of 2018*[74] the committee requested the minister's advice as to the effect of Schedules 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;[75]
- 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;[76]
- 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;[77]

---

73 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

74 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

75 Schedule 2, item 49, proposed paragraph 27E(2)(b).

76 Schedule 2, item 49, proposed paragraph 27E(2)(e). Schedule 3, item 3, proposed paragraphs 3F(2A)(c) and 3F(2B)(c); item 6A, proposed paragraphs 3K(5)(c) and 3K(6)(c). Schedule 4, item 4A, proposed paragraph 199(4)(c); item 5, proposed paragraph 199B(2)(c).

77 Schedule 2, item 49, proposed subsection 27E(5). Schedule 3, item 3, proposed subsection 3F(2C); item 6A, proposed subsection 3K(7). Schedule 4, item 4A, proposed subsection 199(4B); item 5, proposed subsection 199B(3).

- 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;[78]
- 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.[79]

Minister's response

2.141 The minister advised:

> *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'.*[80] 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.

78 Schedule 3,item 3, proposed paragraph 3F(2B)(v) and item 6A, proposed subparagraph (6)(a)(v).

79 Schedule 3, item 2, proposed section 3CAA.

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

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 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.

Committee comment

2.142 The committee thanks the minister for this response.

No requirement to alert occupier before executing warrant, or to consider privacy implications for third-parties; and no prohibition on copying third-party data

2.143 The committee notes the minister's advice that given the covert nature of surveillance, in many circumstances it would not be appropriate to notify a third-party occupier before executing a computer access warrant and there could be significant risk if third parties were required to be notified. The committee also notes the minister's advice that access to third party premises must be considered by the judge or AAT member and as such is pre-authorised by an independent party and not at the discretion of an authorising officer.

2.144 The committee also notes the minister's advice that in authorising activities under a warrant that may impinge on the privacy of third parties, the judge or AAT member would have already have had to, as part of the broader warrant, considered the privacy of any person under proposed paragraph 27C(2)(c).

2.145 The committee further notes the minister's advice that the copying of third party data is only permissible where it would be evidentiary material or is necessary for the execution and concealment of a computer access warrant. The committee notes the advice that prohibiting the copying of information, including third-party data, may critically hinder the ability to replace data to conceal the execution of the warrant. The committee also notes the minister's advice that the judge or AAT member must assess privacy implications when issuing the warrant, although it may be impossible to determine at the outset whose privacy may be impacted. The committee notes that it had sought the minister's advice as to why there was no requirement that copies of third party data be destroyed if it contains no relevant investigative value, but this question was not addressed in the minister's response.

Authorisation to obtain account-based data of third parties

2.146 The committee notes the advice that the transient and mobile nature of cloud communications requires law enforcement to access a range of data associated with the use of a computer. As such, it may be that a computer found during the execution of a search warrant will have had a broad range of persons using that computer or a person of interest is 'using the accounts of others' to conduct illicit activity, and the ease of online access makes strict account associations impracticable.

2.147 The committee also notes the advice that the definition of account-based data includes data in relation to a person of interest which is associated with an account for an electronic service with end-users that is used or likely to be used by the person. As such, access to the account based data of friends, family members or business associates of a person of interest could be accessed as part of this power.

2.148 The committee reiterates it has concerns that the coercive powers in the bill may adversely affect third parties who are not suspected of any wrongdoing. The committee notes that the Schedule 3[81] provisions would authorise relevant law enforcement officers to use a computer found in the course of a search or use a telecommunications facility or other electronic equipment for the purpose of obtaining 'account-based data' in relation to 'a person who uses or has used' the computer found in the course of the search. This would allow the account-based data of *any* person who has ever used the target computer, or the data of third parties who have links with an individual who is the subject of a search warrant, to be accessed by law enforcement officers. No information was provided by the minister as to what use would be made of third party data and what safeguards are in place to protect the privacy of innocent third parties.

2.149 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.150 In light of the information provided, the committee makes no further comment in relation to the lack of a requirement to alert the occupier before executing a warrant, to separately consider the privacy implications for third parties or to copy third party data.

2.151 The committee otherwise draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of obtaining account-based data of third parties who are not the subject of the original search

81 Schedule 3, item 3, proposed subparagraph 3F(2B)(a)(v) and item 6A, proposed subparagraph 3K(6)(a)(v).

warrant, in the absence of information as to the safeguards in place to protect the privacy of innocent third parties. [82]

Coercive powers
Privacy (Schedules 2 to 5)[83]

2.152 In *Scrutiny Digest 12 of 2018*[84] the committee requested the minister's advice as to 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.[85]

Minister's response

2.153 The minister advised:

> 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.

---

82 Schedule 3, item 3, proposed subparagraph 3F(2B)(a)(v) and item 6A, proposed subparagraph 3K(6)(a)(v).

83 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

84 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

85 Schedule 2, item 49, proposed subsection 27A(6).

> 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*.

Committee comment

2.154 The committee thanks the minister for this response. The committee notes the minister's advice that it is imperative that law enforcement can readily determine if a control order is being complied with and so it is necessary and appropriate that this be a basis for issuing a computer access warrant.

2.155 The committee reiterates that it is an offence to contravene a control order, punishable by imprisonment of up to five years,[86] and as such, an investigation in relation to whether a person has committed the offence of contravening a control order could be investigated under a computer access warrant for offence investigations more broadly. As such, the committee had noted that it was unclear why it is necessary to separately, and on a lower threshold, enable a law enforcement officer to obtain a warrant to determine if a control order is being complied with. As such, the committee requested advice as to 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. The committee notes the minister's response did not answer the committee's question, other than to say that law enforcement needs to be able to readily determine compliance with an order.

2.156 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of enabling 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).

---

86 Section 104.27 of the *Criminal Code Act 1995*.

Coercive powers
Privacy (Schedules 2 to 5)[87]

2.157 In *Scrutiny Digest 12 of 2018*[88] the committee requested the minister's advice as to 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.[89]

Minister's response

2.158 The minister advised:

> 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.

---

87 Schedules 2 to 5. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

88 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 28-42.

89 Schedule 2, item 119.

Committee comment

2.159 The committee thanks the minister for this response. The committee notes the minister's advice that the government considers it necessary and appropriate to admit evidence generated by a subsequently void control order given the likelihood such evidence will prove serious offences. The committee also notes the advice that computer access warrants are 'uniquely suited to investigating clandestine communications' and so more likely to provide evidence relating to serious terrorism offences.

2.160 The committee notes that in its initial analysis it stated that it was particularly concerned that such information may be used for purposes relating to preventative detention orders (PDOs). PDOs are administrative orders made, in the first instance, by a senior Australian Federal Police member, which authorise an individual to be detained without charge, and without a necessary intention to charge the subject with any offence. The committee considers PDOs raise scrutiny concerns as they permit a person's detention by the executive without charge or arrest. The minister's response did not address this aspect of the committee's concerns.

2.161 The committee reiterates that the use of information obtained in circumstances where a court has declared a control order to be void and of no effect, may have serious implication for personal rights and liberties. The committee notes that if information is obtained as a result of an interim control order that is subsequently declared to be void, the information was therefore obtained on the basis of a legally invalid exercise of power.

2.162 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of enabling the use of information obtained under a computer access warrant granted on the basis of an interim control order which is subsequently declared by a court to be void.

Presumption of innocence: certificate constitutes prima facie evidence (Schedules 2 and 5)[90]

2.163 In *Scrutiny Digest 12 of 2018*[91] the committee requested the minister's advice as to:

90 Schedule 2, items 17, 18 and 119A; and Schedule 5, item 2, proposed section 21A. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

91 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 42-45.

- 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*;
- 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.

Minister's response

2.164 The minister advised:

> Necessity and appropriateness of expanded power to issue evidentiary certificates
>
> 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.

<u>Circumstances where evidentiary certificates intended to be issued</u>

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.

Committee comment

2.165 The committee thanks the minister for this response. In relation to evidentiary certificates under the ASIO Act relating to voluntary assistance, the committee notes the minister's advice that the certificates would only deal with factual matters, and would not deal with questions of law (which would be determined by the court).

2.166 In relation to evidentiary certificates under the ASIO Act relating to concealment activities, the committee notes the minister's advice that the certificates would cover the manner in which evidence was obtained and by whom,

but would not cover the evidence itself. The committee notes the advice that, as a consequence, the court will retain its ability to test the evidence before it. The committee also notes the minister's advice that, 'for operational security reasons', the ASIO Act does not provide a conclusive list of matters that may be included in an evidentiary certificate. The committee also notes the minister's advice that the regime is not intended to allow the prosecution to provide proof of any facts that are central to establishing an offence, without recourse to challenge evidentiary certificates and the facts that they cover.

2.167 In relation to evidentiary certificates issued under the SD Act, the committee notes the minister's advice that the certificates will cover 'mere technical matters' relating to obtaining evidence, but will not relate to the evidence itself. In this respect, the committee notes the advice that certificates issued under the SD Act will protect capabilities by ensuring that prosecutors are not required to disclose mechanical and operational matters related to law enforcement, unless a defendant seeks to challenge the methods used to gather evidence.

2.168 The committee also notes the minister's advice that evidentiary certificates under the ASIO Act and the SD Act would be issued in circumstances where it would be difficult to establish particular matters without exposing sensitive law enforcement capabilities or compromising existing operations.

2.169 The committee further notes the minister's advice that the evidentiary certificates will only extend to sensitive information, and this is necessary to protect the sensitive operating capabilities of law enforcement agencies, and to preserve the integrity of investigations.

2.170 Finally, the committee notes the minister's advice that the defendant will not be prevented from leading evidence to challenge an evidentiary certificate. In this regard, the committee notes the advice that the nature of the regime provides the defendant with the ability to seek to establish that acts undertaken in the execution of a warrant contravened the ASIO Act or the SD Act and that the prosecution would still have to make out all elements of any offence.

2.171 While noting the minister's comprehensive advice, the committee remains concerned that the provisions in the bill relating to evidentiary certificates may impose a significant burden on persons seeking to challenge the validity of certain actions—in particular things done in the execution of warrants and steps taken to conceal them. For example, and as noted in the committee's initial comments, if an evidentiary certificate were to be issued in relation to things done to conceal access to a person's computer under a computer access warrant, a person wishing to challenge the matters in the certificate would be required to raise evidence to rebut them. However, as the matters in the certificate would relate to covert access and concealment, raising such evidence may be extremely difficult.

2.172 Moreover, while the committee acknowledges that certificates may not cover evidence going directly to a person's culpability for an offence, the minister's

response indicates that they may cover how that evidence was obtained. In some cases, the question of whether evidence was unlawfully obtained may be central to whether a person is ultimately convicted of an offence. Consequently, it is not apparent that the evidentiary certificates contemplated by the bill would in all cases be sufficiently removed from the main facts at issue in proceedings—such as would make their use appropriate.[92]

2.173 Finally, while the minister's response indicates that the evidentiary certificate regimes in the ASIO Act and SD Act are not intended to allow the prosecution to prove facts that are central to a person's culpability, the committee notes that there appears to be little on the face of the bill that would limit the use of evidentiary certificates in this manner.

2.174 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of that document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.175 The committee otherwise draws its scrutiny concerns to the attention of senators, and leaves to the Senate as a whole the appropriateness of expanding the circumstances in which evidentiary certificates may be issued under the *Australian Security Intelligence Organisation Act 1979* and the *Surveillance Devices Act 2004*.

Significant penalties (Schedules 2 to 5)[93]

2.176 In *Scrutiny Digest 12 of 2018*[94] the committee requested the minister's advice as to why the committee requested 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.

2.177 The committee also sought 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 suggests the higher penalty is to incentivise a suspect to comply with the order).

---

92 See Attorney General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 55.

93 Schedule 2, item 114, proposed subsection 64A(8); Schedule 3, item 9; Schedule 4, item 18; and Schedule 5, item 3, proposed subsection34AAA(4). The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

94 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 45-47.

Minister's response

2.178 The minister advised:

> 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.
>
> 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.

Committee comment

2.179 The committee thanks the minister for this response. The committee notes the minister's advice that the increased penalties are to bring the penalties in line with the types of offences being investigated under an assistance order. The committee also notes the minister's advice that the increase in penalties is intended to provide an incentive for people who would otherwise consider non-compliance with the order to be a better option (as it would lead to a lower penalty), than to comply with the order which could lead to evidence being found of a crime which may be subject to a higher penalty.

2.180 However, the committee notes that the minister's justification for the penalties is to refer to other type of offences that could be investigated using an assistance order. But no information is given as to whether there are comparable offences of failing to comply with an assistance order and the applicable penalty for that. The committee notes that, by way of example, comparable offences in the United Kingdom for failure to comply with a notice to disclose a key to a computer, provide for two years imprisonment, or in the case of national security or child indecency offences, five years imprisonment.[95]

2.181 The committee also notes that the minister's justification for incentivising compliance depends on if the privilege against self-incrimination is not applicable. However, it is not clear to the committee that it has been established that assistance orders do not engage the common law privilege against self-incrimination. If the privilege is available[96] the committee considers the argument for incentivising compliance would not apply. The committee also notes that the penalties would apply to anyone issued with an assistance order, which would include third parties who are not the subject of the investigation. The minister's response did not address this aspect of the committee's concerns.

2.182 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of this document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the Acts Interpretation Act 1901).

95 See sections 49 and 53 of the *Regulation of Investigatory Powers Act 2000* (UK).

96 The committee notes that the bill itself does not expressly abrogate the privilege against self-incrimination.

2.183 The committee draws its scrutiny concerns to the attention of senators and leaves to the Senate as a whole the appropriateness of setting a significant penalty of five to 10 years imprisonment for a failure to comply with an assistance order, which has not been justified by reference to penalties to comparable Commonwealth offences.

Immunity from liability (Schedule 2 and 5)[97]

2.184 In *Scrutiny Digest 12 of 2018*[98] the committee requested 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.

Minister's response

2.185 The minister advised:

> 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

97 Schedule 2, item 119A and Schedule 5, item 2. The committee draws senators' attention to these provisions pursuant to Senate Standing Order 24(1)(a)(i).

98 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 27-28.

> 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.

Committee comment

2.186 The committee thanks the minister for this response. The committee notes the minister's advice that the immunities that would be conferred or extended by item 119A of Schedule 2 and item 2 of Schedule 5 have been included as the possibility of liability would dis-incentivise compliance with authorisations to test interception capabilities and with ASIO's power to request assistance. The committee also notes the advice that the risk of liability may prevent individuals from voluntarily furnishing ASIO with information.

2.187 The committee further notes the minister's advice that there are significant limitations on the scope of the immunities. In this respect, the committee notes the advice that the immunity extended by proposed paragraph 313(7)(caa) is limited by the existing purposes for which duties may be imposed under section 313 of the Telecommunications Act. The committee also notes the minister's advice that the immunities in proposed subsections 21A(1) and (5) are not available in relation to criminal activities or conduct which involves significant loss or damage to property, and only extend to the provision of assistance to ASIO in good faith.

2.188 While noting this advice, the committee remains concerned that proposed subsections 21A(1) and (5)[99] would confer broad immunities on persons who provide information and assistance to ASIO, including in circumstances where the relevant conduct is not undertaken in good faith. Despite the minister's advice that the immunities in those provisions only extend to assistance provided in good faith, there does not appear to be anything on the face of the bill that would limit the immunities in this manner. In this regard, the committee reiterates its concerns that the immunities would appear to extend to persons who may deliberately provide defamatory information to ASIO, so long as the person providing the information reasonably believes that the information would assist with the performance of ASIO's functions.

---

99 Item 2 of Schedule 5.

2.189 The committee requests that the key information provided by the minister be included in the explanatory memorandum, noting the importance of that document as a point of access to understanding the law and, if needed, as extrinsic material to assist with interpretation (see section 15AB of the *Acts Interpretation Act 1901*).

2.190 In light of the information provided by the minister, the committee makes no further comment in relation to the immunity extended by proposed paragraph 313(7)(caa) (item 119A of Schedule 2).

2.191 The committee considers that it may be appropriate to amend the bill to, at a minimum, provide that the immunity conferred by proposed subsections 21A(1) and (5) (item 2 of Schedule 5) applies only to actions taken in good faith.

2.192 The committee otherwise draws its scrutiny concerns in relation to proposed subsections 21A(1) and (5) to the attention of senators, and leaves to the Senate as a whole the appropriateness of conferring immunity from civil liability on persons who provide information and assistance to ASIO, including in circumstances where the relevant conduct is not undertaken in good faith.

Veterans' Affairs Legislation Amendment (Omnibus) Bill 2018

Purpose	This bill seeks to amend various Acts relating to veterans' affairs and military rehabilitation to: • enable the Chief of the Defence Force to make a claim for liability for current serving Australian Defence Force members where they have given consent; • enable the Military Rehabilitation and Compensation Commission to obtain information from Commonwealth, State or Territory departments and authorities, and other third parties when determining a claim; and • ensure that exempt lump sum determinations will apply as exempt lump sums from income tests that applies to Department of Veterans' Affairs income support clients
Portfolio	Veterans' Affairs
Introduced	House of Representatives on 20 September 2018
Bill status	Received Royal Assent on 25 October 2018

Coercive powers
Strict liability
Reversal of evidential burden of proof[100]

2.193 In *Scrutiny Digest 12 of 2018*[101] the committee requested the minister's 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).

100 Schedule 2, item 1, proposed section 151. The committee draws senators' attention to this provision pursuant to Senate Standing Order 24(1)(a)(i).

101 Senate Scrutiny of Bills Committee, *Scrutiny Digest 12 of 2018*, at pp. 59-61.

2.194 The committee noted that its consideration of these matters would be assisted if the minister's response expressly addresses relevant principles as set out in the *Guide to Framing Commonwealth Offences*.[102]

Minister's response[103]

2.195 The minister advised:

> 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

---

102 Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, pp. 22-25 (strict liability), pp. 50-52 (reverse burdens) and Chapters 7-10 (coercive powers).

103 The minister responded to the committee's comments in a letter received 21 November 2018. A copy of the letter is available on the committee's website: see correspondence relating to *Scrutiny Digest 14 of 2018* available at: www.aph.gov.au/senate_scrutiny_digest

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.[104]

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 subsection 151(11) is believed to be the last known person with custody or has the care and control of the

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

> 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.[105]

Committee comment

2.196 The committee thanks the minister for this response. The committee notes the minister's advice that the phrase 'any person' was deliberately included in proposed subsection 151(1) to ensure the provision does not inadvertently limit the persons to whom the Military Rehabilitation and Compensation Commission (MRCC) may issue a notice to produce information or documents, or answer questions.

2.197 The committee also notes the minister's advice that this broad inclusionary provision is required to encompass all persons whom the MRCC and the relevant claimant reasonably believe may have custody, care or control of required information or documents. In this respect, the committee notes the advice that information and documents required by the MRCC are critical to determining claims relating to defence-related injuries or death, and the advice that the power to issue notices assists the MRCC in providing fair outcomes in relation to such claims.

2.198 In relation to the imposition of strict liability (proposed subsection 151(10)), the committee notes the minister's advice that information and documents required by the MRCC may be held by third parties such as medical providers and financial institutions, and may be very difficult to access without incurring significant financial costs. The committee notes the advice that, other than making it an offence of strict liability to fail to comply with a notice under proposed subsection 151(1), there is little that can be done to incentivise these third parties to supply information and documents required by the MRCC to properly asses a claim. The committee also notes that strict liability attaches to an offence which is subject to a relatively low penalty of 10 penalty units.

2.199 Finally, in relation to the offence-specific defence (proposed subsection 151(11)), the committee notes the minister's advice that the existence of a reason not to comply with a notice would be peculiarly within the knowledge of the person to whom the notice is issued, and would be significantly more difficult for the MRCC to disprove than for that person to establish. The committee notes the advice that these reasons may include that the person issued with the notice is not the person with custody or control of relevant information or documents.

---

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

2.200 In light of the information provided by the minister and the fact that the bill has already passed both Houses of Parliament, the committee makes no further comment on this matter.

Chapter 3

Scrutiny of standing appropriations

3.1 Standing appropriations enable entities to spend money from the Consolidated Revenue Fund on an ongoing basis. Their significance from an accountability perspective is that, once they have been enacted, the expenditure they involve does not require regular parliamentary approval and therefore escapes parliamentary control. They are not subject to approval through the standard annual appropriations process.

3.2 By allowing the executive government to spend unspecified amounts of money for an indefinite time into the future, provisions which establish standing appropriations may, depending on the circumstances of the legislation, infringe on the committee's terms of reference relating to the delegation and exercise of legislative power.

3.3 Therefore, the committee has determined that, as part of its standard procedures for reporting on bills, it should draw Senators' attention to bills that establish or amend standing appropriations or establish, amend or continue in existence special accounts.[1] It will do so under provisions 1(a)(iv) and (v) of its terms of reference, which require the committee to report on whether bills:

> (iv) inappropriately delegate legislative powers; or
>
> (v) insufficiently subject the exercise of legislative power to parliamentary scrutiny.[2]

3.4 The committee notes there were no bills introduced in the relevant period that establish or amend standing appropriations or establish, amend or continue in existence special accounts.

Senator Helen Polley
Chair

---

1 The Consolidated Revenue Fund is appropriated for expenditure for the purposes of special accounts by virtue of section 80 of the *Public Governance, Performance and Accountability Act 2013*.

2 For further detail, see Senate Standing Committee for the Scrutiny of Bills *Fourteenth Report of 2005*.