Australian Government
Department of Home Affairs

Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Home Affairs Portfolio responses to Questions on Notice.

Index

QoN No.	Title
TOLA/001	Judicial oversight
TOLA/002	The limitations in clause 317ZG of the bill - the meaning of "systemic weakness"
TOLA/003	Consultation Process
TOLA/004	Other industry assistance regimes
TOLA/005	Section 313 of the Telecommunications Act
TOLA/006	Other questions
TOLA/007	Warrants
TOLA/008	Use of these powers by state and territory interception agencies
TOLA/009	Section 313 - in relation to money laundering or a substantial drug importation

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/001*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 1. Judicial oversight.

Asked:

1 Judicial oversight

The Investigatory Powers Act 2000 in the UK provides that a technical capability notice can be issued by the Secretary of State with the approval of a judicial commissioner. There's no similar judicial oversight of the issuance of a Technical Assistance Notice or a Technical Capability Notices in the Bill before the Committee.

(a) In paragraphs 171 to 173 of your submission, you say that the powers in Schedule 1 are different to the equivalent UK powers in the Investigatory Powers Act 2000 – you argue, for instance, that the UK powers are more expansive. You also state in paragraph 173 that "ministerial authorisations like the Attorney-General's ability to issue a [technical capability notice] are an established aspect of the Australian regulatory regime…".

(i) Given that the powers in Schedule 1 are new powers, could you please identity what existing "ministerial authorisations" are "like" the AttorneyGeneral's ability to issue a technical capability notice? Do any of those powers require the Attorney-General to make a judgment about complex technical issues (such as whether a notice would require the creation of a "systemic weakness or vulnerability")?

(ii) Specifically, what is it about Australia that makes a UK-style judicial check on such a power unnecessary?

(b) Clearly, the issuance of a technical assistance notice or a capability notice would require a balancing of complex technical factors. Ultimately, those notices may be issued solely on the judgment of decision-makers at agencies or the Attorney-General (none of whom are likely to be technical experts). How does the bill ensure that ministerial discretion is properly exercised?

(c) What happens in the event that an interception agency and the technical experts employed by a designated communications provider disagree in good faith about whether a technical assistance notice would require the provider to implement a systemic weakness or vulnerability? Putting to one side the question of whether you think that an interception agency would issue a technical assistance notice, would the bill allow the agency to issue a notice in those circumstances?

(d) In the scenario set out in paragraph (c):

(i) Would judicial review through the Judiciary Act 1903 be the only avenue of appeal available to a designated communications provider?

(ii) Given that a designated communications provider may be a small business or even an individual, are you concerned that a person may not be able to afford to make an expensive and resource-intensive judicial review application in those

circumstances?

(iii) In any judicial review application, would the burden of proof fall on the provider? That is, would the designated service provider be required to prove to a court that a relevant notice would require the provider to implement a systemic weakness?

(e) Please assume that the Attorney-General is satisfied that:

(i) the requirements imposed by a technical capability notice are reasonable and proportionate;

(ii) compliance with the notice is practicable and technically feasible; and

(iii) a technical capability notice should be issued to a provider as a matter of urgency (noting that clause 317W(3)(a) provides that the Attorney General is not required to issue a consultation notice if he or she is satisfied that the notice should be given as a matter of urgency).

Please also assume that:

(iv) upon reviewing the technical capability notice, the relevant designated service provider is concerned that the Attorney-General is asking it to build a new systemic weakness or vulnerability into a form of electronic protection;

(v) the provider's technical experts inform the Attorney-General of this but the Attorney-General disagrees; and

(vi) the Attorney-General insists that the notice is valid and that the provider must comply.

In such a scenario, would judicial review through the Judiciary Act 1903 be the only avenue of appeal against the notice for the designated communications provider? If so, what would the provider have to establish in order to successfully appeal such a notice in court and what standard of proof would apply?

Given that a designated communications provider may be a small business or even an individual, are you concerned that a person may not be able to afford to make an expensive and resource-intensive judicial review application in those circumstances?

(f) Relatedly, given the significant costs involved in bringing a judicial review application, are you concerned that it may sometimes be in the best financial interests of a provider to comply with a technical capability notice that it believes – on reasonable grounds and in good faith – would require it to build a systemic weakness or vulnerability? How does the bill address this issue?

(g) The bill would exclude a decision to issue a technical assistance notice or a technical capability notice from the operation of the Administrative Decisions (Judicial Review) Act 1977.

(i) What is the purpose of this exclusion and why is it absolutely necessary?

(ii) Have you considered whether this exclusion may discourage providers from making judicial review applications, given that the remaining avenues of judicial review are likely to be much more time-consuming and expensive?

(iii) Given the urgency of some criminal investigations – particularly those relating to terrorism and child abuse – why isn't it in the interests of agencies to ensure that a judicial review application is resolved as expeditiously as possible? Or to significantly reduce the likelihood of such an application being made in the first place by requiring judicial authorisation and the input of an independent technical expert prior to any notice being issued?

Answer:

(a/i) There is precedence in existing legislation, including national security legislation, for a Minister to authorise the use of powers or make decisions that are similar in complexity, process and magnitude to the issuance of a technical capability notice (TCN) under Schedule 1 of the Bill. Similar to this Bill, these measures do not require judicial authorisation. Some of this legislation also requires the Minister to consider cyber security risks.
The Security of Critical Infrastructure Act 2018 (SoCI) is an example of an existing regime that requires a Minister to make a decision based on their judgement of complex technical issues. SoCI empowers the Minister for Home Affairs to direct the owner or operator of a critical infrastructure asset (which are those assets considered to be critical in the electricity, gas, ports and water sectors) to manage a risk that is prejudicial to security. The Minister may issue a notice to an entity that fails to mitigate an identified national security risk, which may relate to a vulnerability across a sector (i.e. systemic vulnerability). For example, the Minister may issue a direction for an entity to implement additional cyber security measures to guard against data theft or unauthorised access to the asset's control network. Similar to TCNs this power is only intended for use if the Minister is satisfied that the direction is proportionate, consultation has occurred and the impact of the direction has been considered.

Subclause 9(1)(f) of SoCI provides for a rule-making power for the Minister to add new assets to the definition of a critical infrastructure asset. The Minister's decision to require new sectors or subsectors to meet the obligations in SoCI may be based on an increase or creation of systemic weaknesses or vulnerabilities.

Similarly, section 315B of the *Telecommunications Act 1997* (Telecommunications Act) allows the Minister for Home Affairs to give a carrier or a carriage service provider a written direction requiring them to do, or refrain from doing, a specified act or thing within the period specified in the direction. Directions are made in response to a risk of unauthorised interference or unauthorised access to telecommunications networks or facilities – in some circumstances this unauthorised interference may be possible due to systemic weaknesses in the provider's systems. This power is not subject to judicial authorisation.

In effect, these decision-making powers require detailed consideration of the presence of security risks to network infrastructure. The Government already has security expertise that supports these decision-makers in their exercise of these powers. Additionally, Government Ministers will be consulting extensively with industry to increase their knowledge of potential risks or vulnerabilities.

(ii) While there are parallels between the intent of aspects of the *Investigatory Powers Act 2016 (UK)* (IPA) and this Bill, particularly in relation to ensuring assistance from industry can be sort when required, the size and scope of the two pieces of legislation cannot be compared. Unlike the IPA, this Bill does not provide for:

- bulk interception
- bulk equipment interference
- disclosure of communications data
- the retention of data, including internet collection records.
  The vast majority of the powers in the IPA with Australian equivalents are located in separate pieces of established legislation and are supported by their own safeguards including judicial oversight arrangements and independent oversight. For example, the *Telecommunications (Interception and Access) Act 1979* (TIA Act) regulates targeted interception powers and data retention, and the *Surveillance Devices Act 2004* (SD Act) allows for warrants to be issued for data surveillance devices.

The measures in this Bill contain some similarities to the UK technical capability notice provisions however there are significant differences. Notably, the UK technical capability notice framework does not:

- Contain an express prohibition against the building or implementation of systemic weakness or vulnerabilities or an equivalent provision.
- List the obligations that may be set in a notice in primary legislation; this is instead specified through regulations.
- Expressly prohibit the building of data retention, delivery and interception capabilities
- Prohibit the building of a capability to remove a form of electronic protection (i.e. encryption)
- List extensive criteria that go to considerations of reasonableness and proportionality

Given the vast difference in the scope of the IPA Act and this Bill, and the significant differences in the available scope of a TCN, the ‘double-lock’ regime (judicial and Ministerial authorisation) in the UK IPA is not appropriate for this Bill. The powers in the IPA are more expansive and may have more significant impacts on providers than the proposed powers in Schedule 1. Further, the ‘double-lock’ feature is a product of the oversight mechanism applying to other intelligence collection powers in the IPA Act – like interception warrants. Australia already has a regime of judicial oversight that applies to powers used to support Schedule 1 of the Bill.

(b) The decision-makers for issuing a technical assistance notice (TAN) and TCN represent the highest level of authority for such matters and are well equipped to consider the reasonableness and proportionality of any requirements. Importantly TCNs are subject to Ministerial oversight as they can only be issued by the Attorney-General, the First Law Officer of Australia. Similarly, requirements under TANs can only be set by the head of ASIO or an interception agency, or a senior official in their organisation delegated by them. These decision-makers are supported by well-established agency processes and the deep expertise that exists within Government. A TAN cannot compel a provider to do a thing they aren't already capable of doing – therefore a TAN would be leveraging on the existing capabilities of the provider. As has been stated throughout the Department's submission, to meet the decision-making criteria in most cases the decision-maker for a TAN would need to consult with a provider and benefit from their expertise. It will be unfeasible in many circumstances to expect that a decision-maker could be satisfied as to the technical feasibility of a notice, or have genuinely considered the interests of a provider (as is required by 317RA) without having consulted with the provider. The consultation framework under a TCN establishes a formal period by which the Attorney-General can receive and consider technical information by both a provider, technical expert or other relevant party and factor this information into the ultimate form of requirements present in a notice. Information gathered under this consultation process will necessarily go to the decision-making criteria of a TCN. The function and intent of the TAN and TCN framework is to create a mechanism by which sensible, proportionate and mutually agreeable conditions can be set in a notice.

A TCN is centrally administered and, in addition to information received through consultation, expertise would be sourced from the bureaucracy that is designed to support decision-makers like the Attorney-General. These same agencies are relied upon to provide consistent advice on matters related to maintaining national security and protecting Australians from serious crimes.

Importantly, prior to issuing a notice, decision-makers must be satisfied that the requirements in the notice are reasonable, proportionate, practical and technical feasible. Legal requirements also ensure that the types of matters requested need to be consistent with the existing functions of agencies as provided by law and align with key purposes such as safeguarding national security and enforcing the criminal law.

Providers are able to seek judicial review of notices for a broad range of reasons including on the basis that a requirement would create a systemic weakness or vulnerability. Depending on the issuing body, the Constitution and the *Judiciary Act 1903* (Judiciary Act) provides clear avenues for judicial review of the exercise of powers under new Part 15 of the Telecommunications Act. For example:

- Issue of a TAN by a Commonwealth interception agency (i.e. the AFP) or a TCN by the Attorney-General would be reviewable by the High Court due to its constitutional power of review. The Federal Court may also review these powers through the Judiciary Act.

Agencies empowered under Schedule 1 of the Bill are currently subject to extensive oversight by the Commonwealth, State and Territory oversight bodies (please see the list of State and Territory oversight bodies in the answer to the 'consultation' questions). These organisations have a wide remit to inspect and ensure the compliance of all agencies that are empowered under Schedule 1. This includes the ability to conduct compliance inspections on the use of covert and intrusive powers, require the production of agency information, hear complaints about agency activities and report to Parliament. To ensure these existing oversight bodies are able to fulfil their function, paragraph 317ZF(3)(c) creates an exception to the prohibition against unauthorised disclosure for the purposes of complying with existing oversight powers and requirements.

The Inspector-General of Intelligence and Security

The IGIS has extensive powers to oversight the limited functions of ASIS and ASD under new Division 2. The IGIS will oversee the making and administration of ASIO's functions under a TAN and TCN. IGIS functions include powers to obtain information, take sworn evidence and enter agency premises. In their submission to Home Affairs, IGIS acknowledged that their oversight role could include consideration of complaints from providers and others who may be affected by notices and requests. To facilitate IGIS oversight, the use and disclosure provisions in paragraph 317ZF(3)(f) allows disclosure of information about a TAR or TCN to an IGIS official for the purpose of their exercising powers, or performing their functions or duties.

Given the extension in the oversight functions of the IGIS, Home Affairs, with Government and the Attorney-General's portfolio, will monitor the adequacy of IGIS resourcing. The implications on IGIS oversight will rest on the frequency, and manner, in which the new powers may be used.

Ombudsman and integrity bodies

Commonwealth and State Ombudsman, as well as integrity bodies such as the NSW Law Enforcement Conduct Commission have extensive powers to initiate investigations into the activities of the law enforcement agencies empowered under this schedule. The comprehensive ability of state oversight bodies to scrutinise the functions of interception agencies is not obstructed.

(c) As TANs relate to things that a provider is already capable of doing it is difficult to see how a systemic weakness or vulnerability could be built or implemented via a TAN. However if, having gone through all the decision-making criteria, the decision-maker was satisfied that the requirements were reasonable and that no systemic weakness would be introduced then the Bill would allow the agency to issue a notice. This decision would of course be subject to judicial review.

In regards to TCNs - the provision for a technical expert to be mutually appointed for the purpose of determining whether the requirements in a notice would create or introduce a systemic weakness or vulnerability only relates to TCNs. Ultimately, the decision to issue a TCN lies with the Attorney-General. However, prior to issuing a notice, the Attorney-General must consider important issues including whether the notice would require the provider to build or implement a systemic weakness or vulnerability, and the potential impact to industry and the public. The Attorney-General must also consider any submission from the provider which affords the provider the opportunity to justify how the proposed requirements in a notice is likely to create or implement a systemic weakness or vulnerability.

The Government has publically announced that it supports technologies such as encryption which are important for protecting data and communications, and has no intention or legislative power to force providers to build or implement systemic weaknesses. As a result, and practically speaking, it is likely that agencies will continuously engage with the provider prior to the Attorney-General issuing a TCN to ensure that the notice achieves agency objectives, and does not adversely impact the provider and their networks and systems.

If, after consultation and all submissions have been considered, there remains a disagreement about the presence of a systemic weakness then the Attorney-General may issue the TCN, subject to decision-making thresholds. Like TANs these decisions would be subject to judicial review.

(d) In the scenario set out in paragraph (c):

(i) Yes. The original jurisdiction of the High Court remains and the operation of the Judiciary Act would facilitate review of these decisions.

(ii) Subsection 317W (1) requires the Attorney-General to consider any submission from the provider in relation to the proposed requirements in a TCN. This ensures that the Attorney-General gives consideration to any well-founded and legitimate issues and concerns raised, and, if required, vary the requirements in a notice accordingly. This should negate the need for smaller providers to seek judicial review as the notice will reflect any well-founded and legitimate concerns raised in relation to the proposed requirements necessitating the creation or implementation of a systemic weakness or vulnerability.
Practically speaking, it is likely that agencies will continuously engage with the provider prior to the issuance of a notice to ensure that the notice achieves the agencies' objectives, and does not adversely impact the provider and their networks and systems.

Sections 317TAA and 317MAA require decision makers to give advice to providers relating to their obligations under the new powers. This will ensure that providers have a clear understanding of what they are required to do under the notice and is an opportunity to discuss the remedies available.

(iii) Consistent with existing principles, the party bringing the action bears the burden of proof. This Bill does not reverse that position.

(e/i/ii/iii/iv/v/vi)
If the provider deems that a notice will necessitate the creation or introduction of a systemic weakness or vulnerability, then they are able to seek judicial review through the Judiciary Act. The onus of proof lies with the provider who must demonstrate how the requirements in a notice would necessitate the creation or implementation of a systemic weakness or vulnerability. Ultimately, it is a matter for the provider to determine how best to prove that a notice would require the creation or implementation of a systemic weakness or vulnerability. It is then up to the courts to make a judgement as to whether the requirements in the notice are upheld or not.

Paragraph 317W(3)(a) does not provide a blanket removal of the consultation period in situations where a TCN should be given as a matter of urgency. Rather, the provisions ensure the Attorney-General can shorten the 28 day consultation period in proportion to the situation at hand. For example, a shorter timeframe may be required where a capability can be built to prevent imminent harm to the public or where there is a serious risk that material evidence will be lost without the assistance of a provider. Importantly, section 317ZG still applies in these situations meaning that that the Attorney-General cannot arbitrarily force providers to create or implement systemic weaknesses or vulnerabilities.

The framework outlined in the Bill is one of collaboration and consultation prior to the issuance of a TCN. The costs of judicial review would likely only occur on rare, if any, occasions. The Government pays for any capability developed in a TCN. This has a direct parallel for domestic carriers. This Bill is consistent with agency approaches to assistance under section 313 of the Telecommunications Act (we are not aware of any arbitration by ACMA or judicial review of assistance requested under s313). Based on this case history, it is unlikely that requirements will be imposed that are not fully understood and appreciated by providers.

(f) Judicial review is a last resort, following consultation and collaboration with industry. Equally, judicial review is an expensive exercise for Government. TCNs are supported by strong safeguards and limitations to ensure that requirements in a notice reflect the well-founded and legitimate concerns and issues raised by providers, and do not require the provider to create or implement systemic weaknesses or vulnerabilities. Subsection 317W(1) requires the Attorney-General to consider any submission from the provider in relation to the proposed requirements in a TCN. Before any issuance of a notice, either an agency head or the Attorney-General will have considered any well-founded and legitimate concerns raised in relation to the proposed requirements necessitating the creation or implementation of a systemic weakness or vulnerability.

The Government has publically announced that it supports technologies such as encryption which are important for protecting data and communications, and has no intention or legislative power to force providers to build or implement systemic weaknesses. Section 317ZG has been introduced to ensure that providers cannot be required to systemically weaken their systems of electronic protection under a TCN.

(g/i/ii/iii)
The exclusion of judicial review through the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) is consistent with other legislation relating to national security and law enforcement. For example, decisions made under the IS Act, ASIO Act, *Inspector General of Intelligence and Security Act 1986* and the TIA Act that relate to national security and law enforcement matters are not subject to judicial review under the ADJR Act.

Security and law enforcement agencies may require a TCN in order to access appropriate electronic evidence for an investigation that is underway and evolving. It is imperative that a TAN can be issued and used quickly. It would not be appropriate for a decision to issue a TAN to be subject to judicial review under the ADJR Act or merits review as review could adversely impact the timeliness and effectiveness and outcomes of an investigation.

It is difficult to determine whether the inclusion of merits review or other explicit review processes would discourage providers from seeking judicial review. As detailed above, the inclusion of judicial review through the ADJR Act is not best aligned with the Bill's objectives. The Bill does not impede providers' ability to seek judicial review through other means which will provide a sufficient determination as to the legality of the issuing of a notice. The number of providers seeking judicial review will likely be limited because of the strong safeguards and limitations, the existing oversight regimes, the criteria for when a notice can be issued, and the fact that the powers are reserved for senior decision-makers. This gives confidence to providers that TANs and TCNs will not require the creation or implementation of systemic weaknesses or vulnerabilities and that these powers will not be used for arbitrary reasons.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/002*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 2. The limitations in clause 317ZG of the bill - the meaning of "systemic weakness"

Asked:

2 The limitations in clause 317ZG of the bill (in particular, the meaning of "systemic weakness")
A technical assistance notice or technical capability notice must not have the effect of requiring a provider to implement or build a systemic weakness or a systemic vulnerability into a form of electronic protection (see clause 317ZG).
During the hearing on 19 October 2018, you likened the powers in Schedule 1 of the bill to the existing ability of the AFP to ask a locksmith to open a door to a suspect's home to facilitate the execution of a warrant.
However, to open a physical door does not carry with it a risk of automatically opening – or weakening the locks of – other doors. That is, the owner of Apartment B does not have to worry his door becoming unlocked – let alone swinging open – every time the owner of Apartment A unlocks her door. Moreover, if the AFP (for example) obtains a warrant to search Apartment A and a locksmith picks the lock to the front door in order to facilitate the execution of a warrant, it will not make the lock to Apartment B any less secure.
To continue the analogy, one of the main concerns expressed by submitters to the Committee is that, in a digital context, requiring a locksmith to unlock the "door" to Apartment A may carry with it a risk of opening – or weakening – the doors to Apartments B, C, D, E etc. Alternatively, the AFP may require a skilled locksmith to build a new "master key" that could also be used to open the door of every other apartment. Such a key – or the instructions on how to build the key – could fall into the hands of malicious actors.
For these reasons, many submitters are understandably worried that the use of the powers in Schedule 1 of the bill could, if not appropriately constrained and subject to robust safeguards, inadvertently lead to the devices used by most Australians becoming less secure and more vulnerable to criminals.
It appears that the limitations set out in proposed section 317ZG of the bill are designed to address precisely this issue. However, many submitters to the Committee remain worried that:

- the absence of any independent prior approval process (such as a separate warrant requirement); and
- the ambiguity of the terms "systemic weakness", "systemic vulnerability" and "electronic protection" (none of which are defined in the bill),

makes it very difficult to assess the content of those limitations.

(a) Picking up the locksmith analogy, does the AFP and each "interception

agency" for the purposes of Schedule 1 of the bill, currently have the power to require a particular locksmith with particular expertise to open a door for them (noting that technical assistance and capability notices would impose an obligation on a "designated service provider" to provide assistance)?

(b) The Committee understands that the Department was asked to remove the words "into a form of electronic protection" during its consultation with industry. Why does clause 317ZG of the bill still include the words "into a form of electronic protection"? Does this not implicitly leave open the possibility that a notice could require a provider to implement or build a systemic weakness or a systemic vulnerability into something other than "a form of electronic protection"? If not, why not?

(c) Why does the limitation in clause 317ZG not apply to technical assistance requests? Why doesn't the bill explicitly prohibit an interception agency from asking a designated services provider to voluntarily implement or build a systemic weakness or vulnerability into a form of electronic protection? To quote from the submission of Chris Culnane and Vanessa Teague to the Committee, "[i]f an act is not appropriate to be mandated, why is it acceptable to request that same act to be performed voluntarily?"

(d) In paragraph 45 of your submission, you state that "[p]roviders are best placed to understand their services and the technology they work with and are more aware of the technical methods to assist agencies that will not compromise the security of their systems". In light of this recognition:

(i) Doesn't it follow that a provider – and not a senior police officer or Attorney-General – would also be best placed to determine what is and what is not a "systemic weakness or vulnerability" in any given case?

(ii) Why doesn't the bill require interception agencies to even consult with a provider prior to issuing a technical assistance or capability notice?

(e) As noted above, the issuer of a technical assistance notice or a technical capability notice is not required to consult with either:

(i) the relevant provider; or (ii) any independent technical expert, prior to issuing a technical assistance notice or a technical capability notice (noting that, in the case of a technical capability notice, the Attorney-General is not required to issue a consultation notice if he or she is satisfied that the notice should be given as a matter of urgency). As such, how does the bill ensure that the issuer of a notice cannot issue a notice unless it is technically feasible, reasonable and proportionate to do so?

(f) Will there always be a clear bright line between a "systemic" weakness or vulnerability and a "non-systemic" weakness or vulnerability? If so, will the distinction between the two concepts always be clearly evident to a nontechnical expert (such as a senior police officer or an Attorney-General) who is responsible for issuing a technical assistance notice or technical capability notice? If so, how does the bill ensure this?

(g) You assert in paragraph 109 of your submission that the purpose and meaning of proposed section 317ZG and, in particular, the term "systemic" "is clear in the text of the Bill". Would the prohibition on the introduction of systemic weaknesses or vulnerabilities extend to a technical assistance or capability notice that:

(i) ordered a provider to add a new endpoint to an encrypted service that allowed end to end encryption of messaging between multiple endpoints (eg an encrypted system that synched messages between phone handsets, tablets, PCs);

(ii) ordered a provider to introduce a 'Clipper chip' style system in which services were required to use a specific encryption algorithm to facilitate law enforcement decryption;
(iii) ordered a provider to make technical alterations to encrypted services provided to all end users of a service offered by a provider, including the encrypted services offered to end users beyond the scope of a specific warrant/law enforcement investigation;
(iv) ordered a provider to develop a tool that can unlock a particular user's device regardless of whether such tool could be used to unlock every other user's device as well;
(v) ordered a provider to install untested or uncertified software that could inadvertently introduce new systemic weaknesses or vulnerabilities; or
(vi) ordered a provider to disclose vulnerabilities, including systemic vulnerabilities, that have not yet been patched? For example, could an interception agency issue a technical assistance notice to Facebook at the end of every month requiring it to disclose all then-known vulnerabilities in Facebook's systems?

(h) In the public hearing on Friday 19 October 2018, Mr Hansford said that a technical assistance or capability notice that ordered a provider to introduce an encryption key escrow arrangement for an encrypted system would be prohibited by proposed section 317ZG. Why doesn't the bill include a list of examples of "systemic" weaknesses or vulnerabilities, like the introduction of an encryption key escrow arrangement, to better clarify what is meant by the term "systemic"?

(i) A number of submitters have argued that if a tool or method can be developed to apply to one service or device, it can be replicated to other services and devices. If the Attorney-General required a provider to build such a tool or method for an agency, and that tool or method was lost or stolen, would that constitute a systemic weakness for affected services or types of devices for the purposes of the bill?

(j) In the hearing on 19 October, Mr Pezzullo said that the word "'systemic' intrinsically means pertaining to the whole system". Could you clarify what is meant by "the whole system"? Does this mean that a weakness or vulnerability that applied to part of a system – even a large part of a system – would not be a systemic weakness or vulnerability?

(k) To use an example, users of the Facebook app are regularly invited to download new versions of the app (or "updates"). Some users may install the update immediately, while others may take longer or not install the update at all. It may also be possible for Facebook to make different versions of its app available in different countries. For that reason, Facebook's customers may be using different versions of the app at different times and in different places. Would a weakness or vulnerability that is only present in:
(i) an old version of the Facebook app (albeit one that is still used by millions of users); or
(ii) a version of the Facebook app that is used only by Australians, be a "systemic" weakness or vulnerability? Or would each version of the app constitute a different "system"? If so, how does the bill make this clear?

(l) In its submission, the Internet Policy Research Initiative at the Massachusetts Institute of Technology wrote that "[i]t is still an open question whether it is possible to design a secure [exceptional access] system, and in the course of our work at MIT, we have yet to find an [exceptional access] design that would satisfy the requirement of avoiding the introduction of systemic weaknesses or vulnerabilities". Has the Department considered the possibility that it may not yet be possible to

implement or build a weakness or vulnerability into a form of electronic protection that is not systemic? Does the Department disagree with the submission made by Internet Policy Research Initiative at the Massachusetts Institute of Technology? If so, on what basis?

(m) Has the Department been able to identify an exceptional access system that would satisfy the requirements of avoiding the introduction of systemic weaknesses or vulnerabilities? If so, please provide examples.

(n) In their submission to the PJCIS, Chris Culnane and Vanessa Teague of the University of Melbourne argue that "[t]he security implications of a particular proposal are incredibly difficult to understand, even for experts". They go on to cite a number of examples of exceptional access mechanisms that inadvertently introduced systemic weaknesses which were only discovered "when multiple large teams of independent researchers communicated together about the theory and practice of TLS".

In light of the above, Chris Culnane and Vanessa Teague (and a number of other submitters) express concern about the breadth of the prohibition on the disclosure of information relating to a technical assistance request, a technical assistance notice or a technical capability notice in clause 317ZF. In order to allow for a better assessment of the unintended consequences for weakening the security of other users, they recommend that the bill "[i]nsist on full transparency of the methods, while acknowledging that details of particular targets and operations may need to be secret for a while."

Why doesn't the bill provide for full transparency of exceptional access methods that are implemented or developed pursuant to a technical assistance or capability notice while also requiring that the details of particular targets and operations are kept secret? Was this approach considered and, if so, why was it rejected?

Answer:

(a) Section 3G of the *Crimes Act 194* (the Crimes Act) sets out that an officer executing a warrant may obtain such assistance as is necessary and reasonable from a person who is not a constable and has not been authorised to assist in the execution of the warrant. The Explanatory Memorandum to the Crimes Act provides, as an example of the use of this power, "a locksmith assisting the police to open a safe".

Where the AFP has a search warrant to access a premise, a second warrant is not required in order for a locksmith to assist police with opening a door.

The AFP does not have the power to compel a particular locksmith with particular expertise to open a door. However, section 3G(b) of the *Crimes Act 1914* provides that in executing a warrant, police may obtain such assistance as is necessary and reasonable in the circumstances. This provision allows the AFP to find a locksmith with the necessary expertise and willingness to assist. Should no such locksmith be found, the AFP has the power to use such force against things (such as doors) as is necessary and reasonable in the circumstances.

(b) As a consequence of industry consultation the Department changed the wording of the limitation in 317ZG from 'into a form of electronic protection that would make methods of encryption or authentication ineffective' to 'into a form of electronic protection'. This change was well received by providers as it clarified the intent that the legislation does not want to weaken anything that is designed to make devices and systems more secure.

As suggested, the term electronic protection is purposefully broad. An ordinary understanding would allow it to capture passwords, encryption methodology and other security layers and forms of authentication. The Department has not defined it to allow scope for providers to submit and argue that particular features of devices and services do indeed protect the device from unauthorised interference. The Department considered that leaving the limitation at building or implementing a systemic weakness or vulnerability would be unnecessarily ambiguous (what is being weakened?) and the term electronic protection establishes a helpful anchor. Electronic protections are designed to reduce the risk of unauthorised interference with a person's services or devices, therefore weaknesses or vulnerabilities that erode these protections are the relevant ones.

(c) The industry assistance provisions of the present Bill are designed to facilitate cooperation between law enforcement and industry partners. The inclusion of a voluntary mechanism for seeking industry assistance in technical assistance requests is a reflection of the Bill's cooperative intentions. As technical assistance requests are voluntary and, therefore, cannot compel providers to perform any activity whatsoever, they were not considered to require the same safeguards as the notices available elsewhere in the Bill.

Were a provider asked to build a systemic weakness into a form of electronic protection under a technical assistance request they may easily refuse and that ability would be in no way extended by including these requests within the 'backdoors' prohibition of section 317ZG. Further, where a provider does not consider that what they are being asked to do would result in the introduction of a systemic weakness, they are equally capable of proceeding as a result of a request as they would be if the instructions had been contained within a notice.

For these reasons, the Department does not consider it is necessary or desirable to extend the prohibition of section 317ZG to include technical assistance requests.

(d)

(i) Allowing providers the ultimate authority to determine what amounts to a systemic weakness would undermine the compulsory nature of the notices. While providers may possess the most thorough understanding of their systems, it may also be prudent to evaluate these views against the advice of an independent technical expert and government experts, in the case of technical capability notices, and the other concerns identified in the Bill's decision-making provisions.

The consultative mechanisms in the Bill and the decision-making criteria have been established to ensure that the views of providers must be taken into account when setting and evaluating the requirements of a notice.

(ii) When issuing a technical capability notice, the Attorney-General is required to consult with the provider subject to the notice before it is issued under section 317W. Only in very limited exceptions, or with the consent of a provider, can this requirement be waived.

Before issuing a technical assistance notice, the decision-maker must be satisfied that the requirements imposed by the notice are reasonable and proportionate, practicable and technically feasible under section 317P. In considering whether the requirements are reasonable and proportionate, the decision-maker must have regard to the legitimate interests of the designated communications provider to whom the notice relates under paragraph 317RA(c). In most cases, this will necessarily involve consultation with the provider subject to the notice. A failure to consult with the provider, and thus a failure to consider the provider's legitimate interests may result in a notice that is invalid and unenforceable upon judicial review.

Further, it is unlikely that a decision-maker could be genuinely satisfied as to the technical feasibility or practicality of requirements without having consulted with a provider beforehand to gain an understanding of their operations or systems.

(e) The issuer of a technical capability notice is *required* to consult with the relevant provider prior to issuing a technical capability notice under section 317W (except as a matter of urgency). The sum of knowledge that will be gained through expected industry consultation and resident government expertise may, in some circumstances, be sufficient to allay concerns that a technical adviser is necessary. In circumstances where there is disagreement between the Attorney-General and the provider as to whether the notice requires a systemic weakness to be built, an independent technical expert may be consulted under subsection 317W(7).

As detailed above, while a decision-maker is not *required* to consult with the relevant provider before issuing a technical assistance notice, failure to do so may result in the notice being invalid upon review. Given that technical assistance notices can only require a provider to implement existing capabilities and not to construct a new capability, the appointment of an independent technical expert has been confined to TCNs.

Judicial review is available to review any disagreements as to the presence of a systemic weakness that remain unresolved through the consultation and issuing process.

(f) It is conceivable that a single set of instructions could create a systemic weakness when implemented into the systems of one provider and not another. The Bill addresses this issue by leaving 'systemic weakness' to be defined on a case-by-case basis in consultation with providers and, in the case of technical capability notices, independent technical experts. These safeguards ensure that decision-makers will have sufficient information to determine if the requirements of a notice constitute the creation or implementation of a systemic weakness.

In a technologically diverse and complex environment, requirements are best left to examination and treatment on a case-by-case basis, it is not helpful to the purpose of protecting the integrity of systems prescribe rigid assessment criteria.

Were 'systemic weakness' defined by the Bill, it may be impossible to avoid circumstances whereby a particular provider's systems are rendered systemically weaker as a result of a notice without enlivening the prohibition against systemic weaknesses of section 317ZG because of the peculiar nature of a particular provider's systems.

(g) As a general note, the ordinary meaning of 'systemic' will mean that the prohibition captures any requirement that creates a weaknesses that materially impacts electronic protection in a system (which includes interconnecting networks, or a complex whole), as opposed to a particular part. In conjunction with the explanatory memorandum, this makes clear that weaknesses or vulnerabilities into forms of electronic protection that are isolated to a target device or service are not captured by the limitation. This is the assessment that should be made when considering how it will apply to particular hypotheticals.

The decision-making criteria compliments these limitations so that, in addition to considering whether a systemic weakness may be created, providers need to be satisfied of reasonableness, proportionality and impacts on privacy and cybersecurity.

It should be noted that considerable caution should be taken when considering hypotheticals. What is systemic weakness for one system, provider, device or piece of software may not necessarily be so for others.

The express limitations and established decision-making criteria, in addition to the defined purposes for which notices may be issued and the bounded powers of agencies able to exercise the powers are all global factors designed to allow the new measures to be appropriately responsive in a wide-range of investigations. The current drafting is flexible but equally restrained to ensure that mutually agreeable outcomes can be arrived at through consultation with a provider. Hypothetical risks suggested by many submitters seem to misunderstand some of the Bill's measures.

Guidelines will be developed and issued that clarifies decision-making criteria and how this interacts with the concept of systemic weaknesses.

(i) This would likely amount to a systemic weakness and enliven the prohibition of section 317ZG if it created a new endpoint with respect to all users of the encrypted service. However, if the new endpoint was limited to synching information pertaining to a single targeted user and its impacts were limited to that user, then this is unlikely to be prohibited by section 317ZG. It should be clear that to obtain/intercept the communications an appropriate judicially authorised warrant or ministerially authorised warrant would be required.

Further, depending on the nature of a capability to add a new endpoint, it may involve the removal of electronic protection (particularly if done covertly). In this case the limitation for TCNs expressed in section 317T(4)(c)(i) would mean that a TCN could not order its construction.

(ii) This would likely violate the prohibition of section 317ZG. The Department understands that the clipper chip systems allow for a built in and deployed additional avenue of access that presents a material risk of unauthorised use.

(iii) If the ordered alterations rendered the service's methods of authentication or encryption less effective or made the communications protected by those encrypted services open to malicious access, this would likely violate the prohibition of section 317ZG.

(iv) A technical capability notice cannot require the development of a tool that can remove a form of electronic protection (i.e. the locking function on a device) (see 317T(4)(c)(i)).

(v) In order to determine if such an order amounted to the creation of a systemic weakness it would be necessary to determine what the 'inadvertent' consequences of installing the software would be. The decision-maker must be satisfied that the notice will not create a systemic weakness. In a situation where the exact consequences of an action cannot be determined, it is unlikely that the requisite state of satisfaction could be achieved. In this case, the notice will be unenforceable upon judicial review.

A further question would need to be asked – could a senior decision-maker be satisfied that installing untested software on a provider's system that may have serious security consequences is a reasonable thing to do? Consistent with section 317E(1)(c) a TAN would allow for the testing of software before installation in any case, allowing decision-makers to understand the impact of any installation. The prohibition in 317ZG works alongside decision-making criteria and is a factor to consider in any hypothetical posed.

(vi) Requiring a provider to provide information describing existing vulnerabilities in a network would likely not run afoul of the section 317ZG prohibition because it neither causes a provider to implement nor build a systemic weakness. Questions would need to be asked about whether a consistent requirement to disclosure all-know vulnerabilities is reasonable and proportionate, particularly given the scale of Facebook's operations. The ability to intercept and view content is subject to limitations in the existing warrant regime so it is unclear what the utility would be in requiring 'all-known' vulnerabilities to be disclosed, given the targeted scope of the warrants and authorisations required.

In effect such a notification requirement would likely have a positive impact on security – Government support the efforts of providers to make their systems more secure and if providers are aware of vulnerabilities, Government would argue that they should be making a tangible effort to address them.

Further, 317ZG(1)(b) prevents agencies from preventing providers from fixing these weaknesses.

(h) The decision not to exhaustively define 'systemic weakness' in the text of the Bill reflects the understanding that the prohibition will apply differently to different providers.

From the Department's submission to the committee[1]:

> "Given the significant divergence in the sophistication and complexity of systems, the activities that a provider may have to undertake to facilitate access to communications will not be uniform. One provider may be able to meet requirements without creating a systemic weakness, while others may not. The Department considers that the prescriptive, inflexible application of the safeguard carries the risk of creating loop-holes and eroding the global protection it provides."

The Explanatory Memorandum to the Bill does include specific examples of things that would be excluded by the prohibition against systemic weaknesses under section 317ZG. These include placing password rate limits on a device.[2]

[1] Home Affairs Portfolio Submission, pg 20
[2] Explanatory Memorandum, pg 67

(i) A technical capability notice cannot require the development of a tool that can remove a form of electronic protection (i.e. the locking function on a device) (see 317T(4)(c)(i)).

Assuming a hypothetical situation in which the limitation in 317T(4)(c)(i) were not present in the Bill; the existence of such a tool or method would not represent a systemic weakness for the purposes of the Bill.

There is a significant difference between a deployed capability that forms part of a system or device and can be exploited by a malicious actor and a capability that is developed and held in reserve by a provider or agency.

The argument that Government's and industry should not develop the tools necessary to achieve legitimate and important public outcomes, like effective law enforcement or protection of national security, due to a 'risk' that such a capability could be stolen deserves scrutiny. This argument, applied logically across industry, would stymie commercial development and the design and deployment of indigenous agency capabilities. Providers are continually developing new ways of distributing and analysing information. Agencies are progressively improving their investigative capabilities to keep pace with criminality. Each of these parties already hold sensitive information that, if taken by a malicious actor would cause serious concern. However, precisely because the information and capabilities of Government and communications providers are sensitive, there has been significant investment in the development of strong cyber security protocols. Any capability developed consistent with a technical capability notice would be expected to be subject to these same strong protections.

(j) From the Department's submission to the committee[3]:

> "For the purposes of proposed section 317ZG, the term 'system' encompasses interacting or interdependent items that form a unified whole. The term 'systemic' is intended to refer to matters 'relating to a system' rather than a particular part. However, it is not meant to capture systems isolated entirely to a single device, for example.
>
> "Proposed section 317ZG prevents a weakness or vulnerability from being built into a single item (like a target service or device) if it would undermine the security of other, interconnected items. That is, where the weakness in one part of the system would compromise other parts of the system or the system itself. The purpose of the provision is to protect the fundamental security of software and devices and not expose the communications of Australians to hacking. This would capture actions that impact a broader range of devices and services utilised by third parties with no connection to an investigation and for whom law enforcement have no underlying lawful authority by which to access their personal data."

[3] Explanatory Memorandum, pg 67
[3] Home Affairs Portfolio Submission, pg 20

Accordingly the test to consider is not whether the weakness impacts the whole system but rather if it materially degrades forms of electronic protection beyond a target service/s or device/s.

(k)

(i/ii) The introduction of a weakness into an old version of a service or a domestic version of a service that weakens the security available to all users will be prohibited under section 317ZG. The mere presence of such a weakness in an old or domestic version of a service will only interact with section 317ZG insofar as law enforcement cannot prevent the weakness from being patched.

A ‘systemic weakness’ is something that materially degrades forms of electronic protection outside a target device/s or service/s. Such a weakness can be across multiple systems. This is clear in the operation of the Bill which requires decision-makers to be satisfied that the requirements of any notice are reasonable and proportionate and do not require a systemic weakness to be introduced. Where a decision-maker does not recognise that a requirement creates a systemic weakness, providers have the opportunity to raise this during consultation. Where a notice is issued that would require a systemic weakness to be introduced, the decision to issue this notice can be overturned by judicial review. The Explanatory Memorandum to the Bill provides additional guidance on the concept of systemic weaknesses where doubt remains.

(l) This Bill is not an attempt to legislate specific exceptional access systems or to require that providers redesign their entire systems to facilitate Government access. The primary aim of the Bill is to facilitate cooperation between Government and industry at the investigation level, rather than requiring that providers adopt, wholesale, a particular system or device and deploy that across consumers.

The conclusion becomes self-fulfilling where the view is taken that any weakness created is a ‘systemic weakness’ by nature of its existence. Such a proposition is contrary the reality of interception and surveillance capabilities that are used to facilitate warranted access under the existing legislative framework. This Bill will assist in improving the quality, efficiency, timeliness of these capabilities, and the security and integrity of systems by involving relevant DCPs in the process.

Under the present Bill, if a technical capability notice is issued to require that a provider develop a capability that could be utilised across multiple investigations, then that capability is subject to the limitations.

Similarly, on a case-by-case basis where a provider can provide access to information that would benefit an investigation, then the technologically agnostic terminology of the Bill is designed to allow the provider and agency to determine how best that access could be achieved (subject to the limitations). Where a provider does not have sufficient, existing access to the data of its users to be able to assist law enforcement or the ability to gain access without reducing the effectiveness of their electronic protection, they cannot be required to assist.

(m) See above answer (l).

(n) The term ‘exceptional access’ is unhelpful in the context of this Bill – it is commonly used to refer to key escrow schemes, clipper chip designs or other deployed capabilities that impact entire systems or manufacturing chains.

The Bill’s industry assistance framework is technologically neutral and does not introduce ‘exceptional access’ methods into electronic protection. The current form of the industry assistance measures are a direct consequence of the absence of a clear way to provide for secure exceptional access. Without knowing how to implement a widely applied solution, the framework aims to enhance cooperation between agencies and industry to allow them to better work along the sidelines of encrypted technologies and enable access, or achieve other investigatory outcomes.

In addition to the limitation in section 317ZG, other safeguards in the Bill ensure that notices can’t undermine system security. For instance, the Bill does not allow capabilities to be built that allow for decryption or the removal of electronic protection. A TAN, which can compel a provider to do things it can already do, has a very limited capacity to create systemic weaknesses as they would need to be already present in the providers systems.

It remains unclear if it is possible to develop an exceptional access method into an existing form of electronic protection without reducing the effectiveness of the system’s security. It would not be reasonable and proportionate for a decision-maker to compel the introduction of an exceptional access system without understanding how the electronic protection will be affected. Therefore, where this is not understood, this cannot be ordered.

Consistent with long held principles, the Bill’s secrecy provisions are designed to protect commercially sensitive information and the capabilities of law enforcement. Allowing this information to be freely disclosed may harm the interests of providers or instruct bad actors in evading criminal investigations. Exceptions in subsection 317ZF(3) to the unauthorised disclosure offence do allow for oversight of the industry assistance framework by specified Government agencies.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/003*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 3. Consultation Process

Asked:

3 Consultation process
(a) Has the Department specifically identified each State and Territory body that would be responsible for overseeing the use of the powers in Schedule 1 of the bill by State and Territory "interception agencies"?
(b) If so, has the Department approached each of those oversight bodies to ensure that they are appropriately resourced, and have appropriate expertise, to carry out that oversight function in relation to the proposed powers in Schedule 1? If so, when?
(c) Were State and Territory governments provided with a copy of the proposed bill prior to the release of the exposure draft on 14 August 2018? Has the Department explicitly asked State and Territory governments to provide feedback on the form of the bill? If so, who did the Department approach and when? If not, why not?
(d) Has the Department, or the Minister, met with any State and Territory ministers about the form of the bill and, specifically, the industry assistance measures in Schedule 1? If so, who did the Department, or the Minister, meet with? And when?
Note: the purpose of this question is to understand whether the bill introduced into the Parliament on 20 September 2018 has been specifically discussed with State and Territory ministers, and not whether the Department and the Minister have engaged in general policy discussions with State and Territory ministers.
(e) Can you describe the consultations that the Department has undertaken to assess the impact of this Bill on Australian IT exports?
(f) What consultations were undertaken to assess the impacts of this bill on Australian defence licenced exporters?
(g) Was the Defence Industry Department consulted on the form of the bill? If so, when and what did the consultation process entail?
(h) Senetas provides high assurance encryption for government, defence and military data networks. Senetas CEO Andrew Wilson has recently stated in an interview that he believes the bill potentially threatens Australian defence exporters by undermining the trust of international customers in the integrity of encrypted systems sold by Australian companies and creating a perception of supply chain risk (https://risky.biz/RB517/). Indeed, he even indicated that this was a business risk that could potentially force the company to shift its operations overseas.
(i) Has the Department considered an exemption from the operation of the bill for licensed Australian defence exports to address the perception issue raised by Mr

Wilson?
(ii) Why wasn't an exemption of this kind included in the original text of the bill?
(iii) Mr Wilson has also indicated that he believes the formal consultation process for the bill was inadequate and that, while government officials that he had raised this issue with had recognised it as a legitimate concern,
he was "not confident" the concern would be addressed by the government due to the rushed time frame being pursued by the government. Does the Department intend to address Mr Wilson's concern in a revised draft of the bill?
(i) In the hearings on 19 October 2018, you stressed the importance of ensuring that the privacy of innocent Australians is not compromised. Did the
Department consult with the Privacy Commissioner on the drafting of this bill? If so, when did this happen and what did that consultation process entail? Was the Commissioner provided with a copy of the bill as part of that process? If so, when?
(j) In page 3 of its submission to the PJCIS on the Assistance and Access Bill, the Ai Group express concern that the bill "could impact Australia's digital capability and competitiveness, impeding network innovation, discouraging business presence in the Australian market, and leaving Australia behind". Other submitters expressed similar concerns.
Did the Department consider the implications that the proposed industry assistance measures could have on the competitiveness of Australia's technology industry? If so, how? Was a report commissioned on this issue?
(k) Did the Department speak to the Department of Industry, Innovation and Science about the implications that the bill could have for industry competitiveness prior to introducing it into the Parliament? If so, when? If not, why not?
(l) Is the Department satisfied that the bill will have no impact on Australia's digital competiveness or discourage business presence in the Australian market? If so, how did the Department satisfy itself of this?

Answer:

(a) Yes, State and Territory interception agencies are subject to oversight by numerous bodies. These bodies have significant powers to scrutinise the use of investigative powers and broader administrative functions. For example, paragraph 35(1)(h) of the *Telecommunications (Interception and Access) Act 1979* makes it is a precondition to being an interception agency that each State and Territory agency have regular, independent, inspections of their records relating to interception activities. State and Territory also has a general oversight bodies, like Ombudsman, who scrutinise activities and hear complaints. They include:

Jurisdiction	Agency	Oversight body
NSW	**NSW Police**	Law Enforcement Conduct Commission
	NSW Crime Commission	Law Enforcement Conduct Commission
	NSW ICAC	Inspector of the Independent Commission Against Corruption
	Law Enforcement Conduct Commission	Inspector of the Law Enforcement Conduct Commission
Victoria	**Victoria Police**	Independent Broad-based Anti-corruption Commission
	Independent Broad-based Anti-corruption Commission	Victorian Inspectorate
Queensland	**QLD Police**	QLD Crime and Corruption Commission & Public Interest Monitor
	Crime and Corruption Commission	Parliamentary Crime and Corruption Committee & Public Interest Monitor
Western Australia	**WA Police**	Corruption and Crime Commission, Office of the Western Australia Ombudsman
	Corruption and Crime Commission	Parliamentary Inspector of the Corruption and Crime Commission
South Australia	**SA Police**	Office for Public Integrity & Independent Commissioner Against Corruption
	Independent Commissioner Against Corruption	Reviewer of the Independent Commissioner Against Corruption
Northern Territory	**NT Police**	Northern Territory Ombudsman
Tasmania	**Tasmania Police**	Ombudsman Tasmania, Tasmania Integrity Commission

(b) The issuance of a TAR, TAN or TCN where content is required is already subject to existing oversight functions. The technical assistance to obtain support in accessing information can form part of an overall oversight function. This includes but is not limited to the State and Territory integrity bodies and respective Ombudsman's. Some oversight bodies have been consulted in the context of developing the legislation through the Interception Consultative Committee.

Commonwealth oversight bodies like the Inspector-General of Intelligence and Security (IGIS) have noted that, as they are unable to determine what resourcing will be needed to handle potential complaints associated with the Bill, resourcing requirements will need to be monitored (Estimates 23 October 2018 – Legal and Constitutional Affairs Legislation Committee). On a broader noted, the IGIS stated that as the technical environment becomes more complex they will continue to monitor whether their current appropriations for oversight are adequate.

(c) Yes. The Department has consulted with State and Territory agencies extensively on the Bill's provisions. The framework and intent of the Bill was discussed with members of the Interception Consultative Committee (ICC) late in 2017. The ICC includes all interception agencies with powers under the Bill and is a forum to discuss issues related to telecommunications interception, including loss of access to communications caused by encryption and other developments.

An exposure draft was distributed to State and Territories agencies on 11 July 2017 which was discussed in detail on 16 July 2017 via teleconference. The Department then hosted a meeting of the ICC in Canberra on 2 August 2018 to discuss the details of the exposure draft again. At all stages of this process, the Department invited and sought feedback on the form of the Bill. Specific discussions were also had with the NSW Department of Justice, primarily focused on Schedule 2 of the Bill.

(d) No. Consultations with States and Territories were channelled through the key stakeholders on the ICC who have access to the powers. ICC agencies may have briefed their respective ministers.

(e) The Department has discussed the Bill's provisions with key domestic technology providers. Some discussions and their submissions touched on concerns about the supply chain and exports. Impact on IT exports was also raised by some submitters in the public consultation process which the Department reviewed and considered.

These provisions are an ad hoc power and will not require all providers captured to build or implement a capability. The powers have no scope to require an exporter to compromise the security of a range of products. In addition, the limitations on systemic weaknesses, decision-making thresholds, the need to be relevant to the functions or powers of Australian agencies and the requirement for a jurisdictional nexus to Australia restrict the ability for a technical capability notice to impact exported items. If one is required then they as a company can disclose the fact that they have received one on a corporate transparency report.

(f) The Department consulted the Department of Defence on the policy proposal through usual Government processes. However, the Department did not undertake consultations to assess the impact on Australian defence licenced exports. The point above about the limited capacity to impact exports applies to this response as well.

The Department received a public submission from Senetas which mentioned defence export interest.

(g) The Department is not aware of a Defence Industry Department. The Defence Minister and the Department of Defence were consulted on the policy proposal through usual Government consultation processes.

(h) Exemptions for defence exports have not been considered – the powers in the Bill apply to address specific investigative needs and notices will be issued on an ad hoc basis. The deliberation process that underpins notices, as well as the discretionary latitude given to decision-makers allows de-facto exemptions to be granted to the defence industry. Exemptions are more suitable when a regime is in place that applies across the board and where there is little to no discretion as to the application of the powers.

Consideration of an exemption for defence licence exports would imply that the impact on operation of the Bill will effect exports – for the reasons described above the current provisions have very limited scope to do this.

(i/ii/iii) The Department consulted the Office of the Australian Information Commissioner (OAIC) on three separate occasions. This included:

- 22 November 2017 – the OAIC was provided with an early draft of the Bill for comment. On 24 November 2017 the OAIC provided high-level feedback which was considered when finalising the Bill.
- 9 August 2018 – the former Minister for Law Enforcement and Cybersecurity met with OAIC as part of target industry consultations on the Bill. The OAIC was provided with an exposure draft of the Bill along with extensive explanatory materials to assist with their scrutiny.
- 3 September 2018 – the Department met with the OAIC to discuss their concerns with an updated exposure draft of the Bill which was released on 14 August 2018. This exposure draft included changes based on feedback from targeted industry consultation.

(j) Yes. The Department considered the impact of the overall reform package and its regulatory impact on Australian business. As a result, the Bill includes significant safeguards and limitations to minimise the impact to the competitiveness of Australian technology services and products.

The consultation requirements and decision-making criteria that have been discussed already in this response ensure that decision-makers must consider the views of industry. For example, section 317ZAA further narrows considerations of reasonableness and proportionately for TCNs to the legitimate interests of a designated communications provider and a TAN or TCN must be revoked if the decision-maker no longer considers compliance to be reasonable or proportionate (see 317Z for instance). These processes allow feedback about any impacts of specific requirements on the technology industry to be factored into the issuing process.

Requirements under the proposed powers will be tailored to respond to specific circumstances – it is unfeasible to restrict these to a rigid pre-defined set of conditions that are not suited to the dynamic nature of investigations. Rather, the more prudent regulatory approach is to establish global safeguards and decision-making criteria that allow for factors, like the impact on competitiveness, to be determined with reference to the context of the notice. This a key reason why consultation forms part of the regime and why the interests of providers must be explicitly considered and weighed against other factors, like national security and privacy.

A report has not been commissioned at this stage because the Government has engaged directly and extensively with industry stakeholders throughout the development and finalisation of the Bill. As a result, the Bill addresses many of the legitimate concerns raised by industry during confidential and public consultations. Further, many industry concerns are based on a mischaracterisation of what the Bill does. For one, the Bill doesn't not allow for the creation of systemic weaknesses into a form of electronic protection that could compromise exports. Irrespective of this, the Bill applies to both Australian and offshore providers, so long as their activities to have a connection to things *in* Australia. As noted elsewhere, it is difficult to see how lawful capabilities could be built under the scheme that would impact the security of domestic products, let alone exports. The latter would run afoul of the jurisdictional nexus established by section 317C.

(k) The Department did not directly engage with the Department of Industry, Innovation and Science during the development of the Bill. Instead, the Government consulted with key industry stakeholders on the policy intent of the Bill, and an exposure draft of the Bill from July 2017 up until the Committee's review. This engagement occurred at a Ministerial and Departmental level and provided sufficient opportunity for these stakeholders to detail the potential impact of the Bill to their industry. The Bill addresses the proportionate and legitimate concerns and issues raised by industry including those relating to competitiveness.

(l) The Bill actually levels the playing field between domestic and foreign providers by rectifying an arbitrary distinction in current law that sees domestic providers subject to assistance obligations despite the fact that the relevant communications services, devices and components are increasingly supplied and managed by offshore companies. In this way the regime actually improves competitiveness.

Given the framework within the Bill is consistent with other countries the Bill is not likely to discourage business presence in the Australian market.

The Department is not aware of a 'mass exodus' as a result of the Technical Capability Notices within the *Investigatory Powers Act 2016* (UK). These notices can be issued to a wide range of operators that offer or provide a telecommunications service to persons in the UK, whether or not they are in fact in the UK themselves. Given more limited capacity of the Bill's TCNs in comparison (no decryption capabilities, no interception capabilities, more robust decision-making criteria to name a few) they would also not be expected to discourage business activity.

Further, the Bill does not establish default requirements, but rather allows requirements to be tailored to the needs of both agencies and providers as circumstances require. Explicit consideration of impact to industry, in addition to other decision-making criteria and other safeguards in the Bill (i.e. no systemic weaknesses) also limit the impact on competitiveness and businesses operating in the Australian market.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/004*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 4. Other industry assistance regimes

Asked:

4 Other industry assistance regimes
(a) In paragraphs 37 to 40 of your submission, you state that the bill ensures that Australia implements a number of key principles that were agreed between the "Five Eyes" countries. You also note that a number of overseas jurisdictions, including the UK and New Zealand, also have laws directed at securing industry assistance.
Did the Department seek any advice from, or otherwise consult with, the governments of other "Five Eyes" countries, or any other jurisdictions, about how they have dealt with the challenges posed by encryption and, in particular, obtaining industry assistance? If so, what did those consultation processes entail?
(b) In paragraphs 169 to 172 of your submission, you set out a very high level four paragraph comparison between Schedule 1 of the bill and the industry assistance provisions in the UK's Investigatory Powers Act 2016.
Did the Department conduct a comprehensive analysis of the UK powers prior to introducing the bill into the Parliament? Did the Department consult with any experts on the equivalent industry assistance regime in the UK? If so, when did the Department do this and what did that consultation process entail?
Is the Department aware of how, and how often, the power to issue a "technical capability notice" under the UK's Investigatory Powers Act 2016 has been used? If so, please provide details.

Answer:

(a) "Five Eyes" countries were kept informed of the intentions and directions of the Bill through its drafting and received exposure drafts of the legislation up to and including at the Ministerial level through the Five Country Ministerial Meeting. This approach is consistent with the interest of other "Five Eyes" concerning the problems of, and possible solutions to, the challenges posed by ubiquitous encryption. The Department sought knowledge from the UK in regards to the legal effect and operation of their regime, including how industry responded to the development and inclusion of technical capability notices in the *Investigatory Powers Act 2016 (UK)*.

(b) The Department conducted a detailed analysis of the UK powers prior to introducing the Bill into the Parliament. This involved legally trained Departmental officers scrutinising the operation of the UK powers, compiling briefing on that operation and liaising with our counterparts in the UK.

The Department did not consult with independent experts outside the UK Government on the operation of the UK powers. However, the Department consulted with companies experienced in the UK provision during all three stages of the consultation period. This consultation involved formal discussion about their experience with the UK provisions, including while they were being drafted, and their understanding of its effect.

The Department has been advised that information pertaining to how, and how often, the power to issue a “technical capability notice” under the UK’s *Investigatory Powers Act 2016* has been used, is confidential. As a result, the Department is not aware of these details. The Department does not consider obtaining this information to be of particular value because the purposes of each power in the IPA Act and our legislation are distinctive.

The Department cannot make a direct comparison between our legislation and the size and scope of powers in the IPA Act. TCNs under the IPA Act may require the removal of electronic protections or the construction of core capabilities such as an interception capability. TCNs in this Bill cannot require industry providers to build a systemic weakness or other capabilities that make systemic forms of encryption or authentication less effective.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/005*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 5. Section 313 of the Telecommunications Act

Asked:

5 Section 313 of the Telecommunications Act

(a) In paragraph 28 of your submission, you state that "[s]ection 313 of the Telecommunications Act is … ambiguous" and that "[t]his has led to uncertainty in its application and, in many cases, has meant that law enforcement has not been able to receive the help needed". You go on to state that "providers have been willing to assist for a terrorism incident but, in some instances, have not afforded the necessary assistance in relation to money laundering or a substantial drug importation".

Section 313(3) of the Telecommunications Act imposes an obligation on a carrier or carriage service provider to give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the purposes of enforcing the criminal law and laws imposing pecuniary penalties.

(i) Specifically, how many times has a carrier or carriage service provider refused to provide necessary assistance to law enforcement having been asked to do so under section 313(3)?

(ii) Noting that compliance with section 313(3) is not voluntary, how many times has a provider been charged for refusing to comply with a request for assistance?

(iii) Given that many of the submitters have argued that many aspects of Schedule 1 of the bill are ambiguous and, in particular, that the scope of the limitations in clause 317ZG of the bill is unclear, why isn't this bill repeating the error you have identified with section 313(3) of the Telecommunications Act in regards to its ambiguity?

(iv) If the bill is passed in its current form, could a carrier or carriage service provider be ordered to provide the same assistance under both section 313(3) and a technical assistance or capability notice at the same time? Wouldn't the concurrent operation of both regimes actually compound the error you have identified with the current regime (being the ambiguity of section 313 of the Telecommunications Act)?

(v) Given that many of the same providers that are currently subject to section 313(3) of the Telecommunications Act have told you that they regard the bill as ambiguous, why do you think they would be more likely to comply with a technical assistance or capability notice than a request under section 313(3) of the Telecommunications Act?

(vi) Given the deficiencies with section 313 of the Telecommunications Act that you have identified in your submission, why isn't it being repealed by this bill? How

does the retention of an “ambiguous” provision that is uncertain in its application “ensure the smooth delivery of industry assistance from Australian carriers and carriage service providers” (as you argue in paragraph 31 of your submission)?

Answer:

(i) The Department understands that requests under section 313(3) are developed on consultative basis, that is, before a formal request is issued the terms and conditions under the request has already been settled upon by the provider and the agency. As such, there are no figures available for the amount of times requests have been ‘refused’; if a provider seems like they will not be amenable (i.e. consider that it is not ‘reasonable’) to providing the type of assistance initially requested then a formal request is unlikely to be made.

(ii) The Department has been advised that there are no incidences of a provider being charged for refusing to comply for a request for assistance. The Australian Communications and Media Authority has not conducted any arbitration or enforcement action in relation to section 313(3).

(iii) The ambiguity in section 313(3) is significant and impacts both agencies and providers. It simply requires that such help that is ‘reasonably necessary’. In effect the Bill unpacks this concept, listing the types of assistance that should be expected in 317E whilst navigating the boundaries between specificity, technical neutrality and being suitable to respond to case-by-case scenarios which arise as a result of wide investigative needs. There is no limitation or protection in section 313(3) with regards to 317ZG and, while the presence of such a limitation naturally attracts curiosity about its operation, the fact that it is there narrows the range of possible requests when compared to section 313(3).

Questions about comparative ambiguity based on the feedback from submitters should be treated carefully. Many submitters are unfamiliar with section 313(3) and have not been subject to its requirements. Further, the very fact that the Bill introduces further transparency into the operation and effect of industry assistance by introducing a more comprehensive framework means that there is more to scrutinise. Given the scope of entities under the Bill and acknowledging the current limitations in section 313(3), new limitations and greater certainty has been introduced to industry assistance frameworks.

For an ad hoc framework designed to be operationally useful in a number of investigative scenarios, applying to a number of different providers and agencies there will always need to be an element of flexibility.

(iv) Section 313 of the Telecommunications Act encompasses a broad range of agencies – defined as “officers and authorities of the Commonwealth and of the States and Territories” – that are excluded from Schedule 1, such as the Australian Competition and Consumer Commission, sporting integrity bodies and councils. The agencies able to issue compulsory notices under the Bill have been narrowed to interception agencies and ASIO.

The Department is unsure what utility would come about by seeking the same assistance under both provisions – this would seem to lead to unnecessary confusion. Further, a TAN or TCN issued with a section 313 request on foot would arguably not be reasonable or proportionate.

Concurrent operation of Section 313 and the proposed powers in Schedule 1 will ensure the transition of industry assistance from Australian carriers and carriage service providers to the broader range of entities that may seek assistance.

(v) The Bill contains several measures to ensure that requirements are reasonable, practicable and technically feasible. The fact that these terms are set by the decision-maker and not to a contested objective standard creates greater certainty of application. Further, the greater specificity of things required in 317E established an important reference point for the types of assistance that Parliament has deemed suitable. Finally, the more robust process requirements (e.g. notice issue, expiry, variation, form) create a clearer reference point from receiving, complying with, or challenging a request than the nebulous obligations under section 313.

(vi) Section 313 of the Telecommunications Act allows a much broader range of agencies to seek assistance from carriers and designated communication providers that are excluded from issuing compulsory notices under Schedule 1.

Repealing section 313(3) would remove an important mechanism for assistance for many Commonwealth, state and territory authorities. While the decision was made not to invest these authorities with new Schedule 1 powers (given the scope of providers captured by Schedule 1), assistance under 313 remains important for their legitimate functions.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/006*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 6. Other questions

Asked:

6 Other questions

(a) According to the Explanatory Memorandum, the bill is needed to address threats by terrorists, child sex offenders and criminal organisations that use encryption and other forms of electronic protection to mask illegal conduct. As such, why does the bill permit an interception agency (among others) to compel a provider to do an "act or thing" in relation to the enforcement of any criminal law or any law imposing a pecuniary penalty? What is your response to the Law Council's recommendation that the bill be limited to the enforcement of serious criminal laws in Australia?

(b) The definition of "designated service provider" extends to individuals and entities that are not constitutional corporations. Moreover, a provider may be compelled to do an "act or thing" in relation to the enforcement of any criminal law or any law imposing a pecuniary penalty (not just laws with a federal aspect). Has the Department sought legal advice on whether the laws proposed in Schedule 1 are constitutional? If not, why not? If so, what did that advice say and would the Department be prepared to publish that advice in full?

(c) During the public hearing on 19 October 2018, one witness (John Stanton) expressed concern that there had been "authority creep" in relation to the metadata retention laws that were introduced in 2015 (being the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015) ("Interception and Access Bill").

In order to allay public concern when the Interception and Access Bill was passed, access to metadata was restricted to 22 specific police and intelligence agencies, such as the Australian Federal Police, ASIO and state police forces. During the PJCIS public hearing on 19 October 2018, Mr Stanton claimed that there are now many more than 22 agencies that are using their own state-based powers to request metadata from companies.

As of 19 October 2018, how many Australian federal state and territory agencies:

(i) are authorised to access metadata under the Telecommunications (Interception and Access) Act 1979; or

(ii) have the power to access metadata in the manner permitted under the Telecommunications (Interception and Access) Act 1979 under different laws (such as under a law of a State or Territory)? In your answer, please provide details of any similar State and Territory legislation.

Answer:

(a) The proposed Bill has not been framed solely to address threats from terrorism, child sex offenders and criminal organisations. Paragraph 4 of the Explanatory Memorandum also identifies, in addition to the above stated harms, the occurrence of "other crimes" as the result of law enforcement's degraded intelligence capabilities. The harms selectively identified in the question are illustrative of areas intended to be addressed by the Bill but it is nowhere stated that they represent an exhaustive accounting of the crimes that may be investigated under the Bill's new powers, or the existing powers under the TIA Act or SD Act.

The Law Council's recommendation is not feasible. The Bill already includes sufficient limitations on the provision of new powers. In addition to comprehensive decision-making criteria the Bill ensures that the powers cannot be used for purposes not related to established relevant objectives. The Bill's interpretation of a relevant objective is reflected in section 313 of the Telecommunications Act, and in Chapter 4 of the *Telecommunications (Interception and Act) 1979*. The requirement of a relevant objective is not unique, and has proven suitable in addressing the investigative needs of agencies to date. The providers covered by the Bill are required to have a jurisdictional nexus to Australia. This limits assistance requested to matters relevant to Australian authorities. Additionally, notices must be consistent with the powers or functions of the relevant agency to be exercised. These agencies are the core criminal law enforcement and security agencies of Australia – they have set and limited functions and devote their resources according to the most pertinent law enforcement and security priorities of the day.

Further, the powers cannot be used for anything for which a warrant or authorisation is required. A telecommunications interception warrant is still necessary to access the content of communications. This means that when the notices are used to facilitate access to content, the investigation will necessarily be into a 'serious offence' (subject to the seven year threshold under the *Telecommunications (Interception and Act) 1979*). However, it is not only in the execution of interception or surveillance device warrants that these powers may be used legitimately used. Authorisations for communications data for example must satisfy criteria similar to the relevant objectives in the Bill before disclosure. The broader range of providers in the Bill, including carriers and carriage service providers, may be able to undertake activities that allow for the smooth execution of these authorisations. Restricting the operation of these purposes to misalign them with authorisations for communications data is just one example of how a more limited definition could hamstring their ability to assist in the facilitation of other legitimate investigative powers.

As the Explanatory Memorandum affirms, pecuniary penalties in this provision are not intended to encompass small-scale administrative fines. In the Bill, pecuniary penalties relates to breaches of Commonwealth, State and Territory laws that are not prosecuted criminally or impose a penalty which serves as an administrative alternative to prosecution. In Commonwealth, State and Territory legislation there are significant pecuniary penalties for serious breaches of the law. It would be an oversight for the Department to constrain the scope of the Bill to only include 'serious criminal laws'.

(b) Yes, the Department did seek legal advice on the laws proposed in Schedule 1 and was advised that they were constitutional. Accordingly, the Department is satisfied with the constitutionality of the measures. Consistent with standard practice, the Department will not disclose legally privileged advice beyond the necessary Government stakeholders.

(c)

(i) Twenty-two agencies are authorised to access metadata. This includes, the Australian Federal Police; a Police Force of a State; the Australian Commission for Law Enforcement Integrity; the ACC; the Immigration and Border Protection Department; the Australian Securities and Investments Commission; the Australian Competition and Consumer Commission; the Crime Commission; the Independent Commission Against Corruption; the Law Enforcement Conduct Commission; the IBAC; the Crime and Corruption Commission; the Corruption and Crime Commission; the Independent Commissioner Against Corruption and the Australian Security Intelligence Organisation.

(ii) Section 280(1)(b) of the Telecommunications Act enables limited access in accordance with Commonwealth, State and Territory Laws where that lawful access is not in connection with the functions of an enforcement agency. This means that an enforcement agency must either have a warrant to access information or use the authorisation process under the TIA Act.

The inclusion of 280(1)(b) is designed to allow telecommunications providers to disclose data in response to subpoenas or court orders (not in connection with civil proceedings) or the notice to produce powers of a broader range of Commonwealth, State and Territory entities.

Section 280(1B) was inserted by the Data Retention Act in 2015 to ensure that data retained for the purposes of the new data retention regime could not be used in response to subpoenas or court orders in civil proceedings.

The agencies that can access metadata under the TIA Act remain identical to those that were able to obtain data immediately after the passage of the Data Retention Act. Section 280 is an avenue for metadata in response to the established and approved notice to produce powers of Australian authorities, including Courts. The Data Retention Act limited an additional channel, internal authorisations in the TIA Act, to set 22 agencies, but given the legitimate need for disclosures of the information through other avenues did not remove the exception against the prohibition to disclose in section 280. This exception was narrowed by the Data Retention Act to exclude civil proceedings – the decision to do so being subject to a public review (the report on which was released in April 2017).

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/007*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 7. Warrants

Asked:

Thank you. Obviously, we just cleared up some terms before we got into the discussion. I'd also like to touch on warrants. Could you explain, Commissioner, to the general public how a warrant is served, the particulars of a warrant and the duration, because I think it goes to the heart of this bill, if we're going to take the tweezer analogy that the director-general offered in his opening statement.

Answer:

The table on the next page outlines the threshold, authoriser and duration of warrants, authorisations and section 313 notices.

In terms of the process for obtaining a warrant, AFP members must:

1. Prepare an affidavit. The affidavit must outline information such as the type of offence being investigated, how the privacy of any person is likely to be affected, and why the warrant is necessary. The AFP member must then have the affidavit reviewed and approved internally.

2. Make an appointment with a Judge or AAT Member to have the warrant approved. The AFP uses this appointment to provide the Judge or AAT Member with further context on the investigation.

3. For a warrant issued under the *Telecommunications (Interception and Access) Act 1979* (except under section 48), the AFP is required to provide a copy of the warrant to the carrier/carriage service provider.

4. If the warrant needs to be extended or varied at any point, the AFP member will need to prepare a new affidavit and present this, alongside the original warrant, to a Judge or AAT Member for their approval.

In terms of the process for obtaining an authorisation, this can differ depending on the type of authorisation. By way of example, for a prospective data authorisation, AFP members must:

1. Prepare an authorisation form and supporting documents. These must outline information such as how the authorisation will assist the investigation and whether any interference with privacy is justifiable and proportionate.

2. Consider whether there is a reasonable belief the person to whom the authorisation relates is a journalist. If so, a journalist information warrant is required and a different process must be followed.

3. Have the authorisation approved by an authorised officer (Superintendent or above).

4. The AFP must then notify the relevant provider of the authorisation.

5. The authorisation must be revoked if satisfied that disclosure is no longer required.

Threshold	Authoriser	Duration
Telecommunications (Interception and Access) Act 1979		
Telecommunications intercept warrants (audio and data)		
- Offences of 7+ years (plus certain other offences including terrorism)	- Judge or AAT Member	- Up to 90 days, or 45 days for a B party warrant
Stored communications warrants		
- Offences of 3+ years	- Judge or AAT Member	- Warrant is in force until it is first executed or until the end of the period of 5 days after the day on which it was issued
Historical data authorisations (subscriber, call charge records, internet metadata)		
- Enforcement of the criminal law - Locating missing persons - Enforcement of law imposing a pecuniary penalty of protection of public revenue - Enforcement of criminal law in a foreign country *NOTE: For journalists the AFP must first obtain a journalist information warrant from a Judge or AAT Member. Applications for a journalist information warrant are also subject to scrutiny by a Public Interest Advocate.*	- Internally authorised	
Prospective data authorisations (future call associated data [no content] – calling id's, date, time and location)		
- Offences of 3+ years - At request of foreign country for offences of 3+ years following a formal mutual assistance request approved by the Attorney-General *NOTE: For journalists the AFP must first obtain a journalist information warrant from a Judge or AAT Member. Applications for a journalist information warrant are also subject to scrutiny by a Public Interest Advocate.*	- Internally authorised	- Unless revoked, up to 45 days, or up to 90 days where authorisation is made under a journalist information warrant
Surveillance Devices Act 2004		
Surveillance device warrants (listening, tracking, optical and data)		
- Offences of 3+ years	- Judge or AAT Member	- No more than 90 days, or 21 days if issued for the purposes of an integrity operation

Threshold	Authoriser	Duration
Tracking device authorisations (where no trespass)		
- Offences of 3+ years	- Internally authorised	- Up to 90 days
Telecommunications Act 1997		
Section 313 reasonable assistance		
Australian carriers/carriage service providers must give such help as is reasonably necessary for: - Enforcing the criminal law and imposing pecuniary penalties - Assisting the enforcement of the criminal laws in force in a foreign country - Protecting the public revenue - Safeguarding national security	- Internally authorised	

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/008*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Telecommunications and Other Legislation Amendment (Assistance & Access) Bill 2018 - 8. Use of these powers by state and territory interception agencies

Asked:

Perhaps I'll finish by asking you to take this on notice. Could the department identify for the committee each state and territory body that would be responsible for overseeing the use of these powers by state and territory interception agencies?

Answer:

Please refer to QoN TOLA/003 (a).

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 23 October 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/009*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY
Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - 9. Section 313 - in relation to money laundering or a substantial drug importation

Asked:

At paragraph 28 of your submission, you say in relation to section 313:
… providers routinely assess reasonableness based on the type of criminality being investigated. As a result, providers have been willing to assist for a terrorism incident but, in some instances, have not afforded the necessary assistance in relation to money laundering or a substantial drug importation.
How many cases are we talking about in those areas? Are you able to assist the committee?
We'd have to take that on notice. Certainly, we see that providers make judgements about, in their mind, what is a serious crime and what isn't, and what they want to assist us with and what they don't.
Have you had instances where you haven't been able to bring somebody engaged in money laundering or drug importation to justice as a result of section 313 not being adequate for your purposes?
I'm certain the answer to that question is yes, but let us get some details and give you numbers and some cases.

Answer:

The AFP takes a collaborative and consultative process to the issuing of section 313 notices.

This means that as a matter of practice, the AFP will only issue a section 313 notice where the carrier/carriage service provider has requested a section 313 notice to formalise the form of assistance they have agreed to, following a negotiation.

In the interests of maintaining this collaborative and consultative relationship, the AFP will not issue a carrier/carriage service provider with a section 313 request without first discussing the proposed assistance with them. Additionally, the AFP will not issue a section 313 request unless the carrier/carriage service provider has first agreed to provide assistance and has specifically requested the section 313 notice to cover the assistance.

In some instances carriers/carriage service providers have refused to provide assistance based on their subjective view of the seriousness of the offences under investigation. This is best demonstrated by way of the following example-

- The AFP was investigating a large scale importation of illicit substances via a transnational syndicate. The AFP was aware that a particular person of interest (POI) was using encrypted communications to facilitate the criminal activities. The AFP sought assistance from the internet service provider to remotely modify settings on the internet service in order to facilitate the installation of a lawfully authorised surveillance device. Despite the internet service provider acknowledging it was technically feasible and that they had previously provided such form of assistance to an interception agency, they stated they reserved such forms of assistance for national security matters and on this occasion would not assist.

- Negotiations with the carrier continued for a number of weeks, however as the carrier would not agree to the assistance, no section 313 notice was issued.

This form of carrier assistance would have been useful for at least six major criminal investigations over the last 12 months, however due to the above ongoing lack of industry support the AFP has not continued to pursue such forms of assistance.