Australian Government
Department of Home Affairs

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

Department of Home Affairs responses to Questions on Notice.

Index

Index	
TOLA/028	General limits re warrants (Q19) - Giving effect to a warrant.
TOLA/029	Specific questions on TCNs (Q20) - Why are TANs required.
TOLA/031	Specific questions on TCNs (Q22) - Offensive capability.
TOLA/032	Definition of DCP (Q23) - Class of designated communication's providers.
TOLA/033	Industry Assistance - Structure (Q24) - Concerns on designated communications.
TOLA/034	Issuing the notice or request - Authorisation (Q25) - Judicial authorization.
TOLA/035	Industry Assistance - Structure (Q26) - Exercise of powers.
TOLA/037	Relevant objective (Q28) - National security.
TOLA/039	Reasonable and proportionate & technically feasible (Q30) - TAN or TCN criteria.
TOLA/040	Reasonable and proportionate & technically feasible (Q31) - Two standards.
TOLA/042	Manner and form (Q33) - Information to be included in the notice.
TOLA/043	Consultation (TCN) (Q34) - Appointment of technical expert.
TOLA/044	Consultation (TCN) (Q35) - Appointment of cost negotiators.
TOLA/045	Consultation (TCN) (Q36) - Consultation mechanism for TCNs (section 317W).
TOLA/046	Variation (Q37) - DCP engagement to vary a TAN or TAR.
TOLA/049	Variation (Q40) - Greater transparency of new capabilities.
TOLA/050	Oversight (Q41) - The Bill's interaction with the Public Interest Disclosure Act 2013.
TOLA/051	Oversight (Q42) - Commonwealth Ombudsman accessing TAR information.
TOLA/052	Oversight (Q43) - OAIC and adverse impact on privacy.
TOLA/053	Oversight (Q44) - Powers under Schedule 1.
TOLA/054	Oversight (Q45) - Oversight mechanisms.
TOLA/056	Oversight (Q47) - Division 6 and DCP communication.
TOLA/057	Oversight (Q48) - Secrecy offences in Division 6.

Index	
TOLA/058	Oversight (Q49) - The offence provision in 317ZA.
TOLA/059	International context - General - (Q50) - Civil or criminal liability overseas.
TOLA/060	International context - General - (Q51) - Proposed powers in Schedule 1.
TOLA/062	International context - General - (Q53) - Conflicts of law.
TOLA/064	Similarities and differences between Schedules 2, 3 and 4 powers - Implementation and guidance to industry - (Q55) - Guidance to industry if Bill passed.
TOLA/070	Similarities and differences between Schedules 2, 3 and 4 powers - (Q61) - Proposed amendments to the Surveillance Devices Act (Schedule 2) warrants.
TOLA/071	Similarities and differences between Schedules 2, 3 and 4 powers - (Q62) - Execution of a search warrant on premises.
TOLA/072	Similarities and differences between Schedules 2, 3 and 4 powers - (Q63) - Schedule 3 proposal re section 3LA(5) of the Crimes Act.
TOLA/073	Similarities and differences between Schedules 2, 3 and 4 powers - (Q64) - Schedule 4 amendment to the existing offence at section 201A9(3).
TOLA/075	Similarities and differences between Schedules 2, 3 and 4 powers - (Q66) - Intention reflected in proposed section 21A of Schedule 5.
TOLA/077	Similarities and differences between Schedules 2, 3 and 4 powers - (Q68) - subsection 21A(1) provides “clear” thresholds.
TOLA/079	Similarities and differences between Schedules 2, 3 and 4 powers - (Q70) - Compulsory assistance order.
TOLA/081	Similarities and differences between Schedules 2, 3 and 4 powers - (Q72) - Paragraph 102 of the Department’s supplementary submission.
TOLA/082	Similarities and differences between Schedules 2, 3 and 4 powers - (Q73) - Method and mode in which compulsory assistance orders must be issued.
TOLA/083	Similarities and differences between Schedules 2, 3 and 4 powers - (Q74) - proposed sections 21A and 34AAA.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/010*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q1) - Explanatory Memorandum

Asked:

1. The Explanatory Memorandum states that 'Schedule 1 introduces a new, graduated approach to industry assistance'.1 The Bill does not require a relevant agency to seek voluntary assistance prior to graduating to a compulsory notice. If voluntary assistance is to be preferred, why does the Bill not require an agency to issue a TAR before compulsive notices are issued?

Answer:

While it is not a requirement that a technical assistance request be issued in the first instance, in practice it is very likely. Both agencies and many providers have consistently expressed the preference to seek, and provide, technical assistance on a voluntary basis. The TAR framework allows for this to occur. It is anticipated that the possibility of issuing a TAR will open discussions with a provider and allow agencies, like the Australian Federal Police, to reach mutually agreeable terms for that assistance. The central premises of Schedule 1 is to establish a framework that allows both Government and industry to cooperate in good faith to reach important public safety outcomes.

During consultation with industry providers noted that, in some cases, legal compulsion for assistance will be necessary to give comfort to providers that they are acting in response to a clear obligation. The desire for a requirement to assist is also consistent with agency experiences with industry to date. Where there is this understanding, or where it is clear that a provider would not voluntarily cooperate, a technical assistance notice may be issued in the first instance. To require a technical assistance request to be issued before a technical assistance notice in these circumstances would be redundant. Given the different preferences of providers, the Department anticipates that the appropriate notice or request type will be determined in consultation with the relevant designated communications provider before any formal instrument is issued.

Further, adding a requirement to seek a technical assistance request before a technical assistance notice could jeopardise the urgent or timely resolution of critical investigative matters. Responding to child abduction cases, situations in which there is serious risk to life or property or circumstances where there is a likelihood that evidence will be destroyed, may require speedy cooperation from industry to ensure that the relevant communications can be accessed or industry expertise can be leveraged. Requiring a formal TAR request that may not be actioned before the legal compulsion could lead to significant harm. The regime as currently drafted enables a graduated approach to be followed in practice but creates enough flexibility to leverage compulsory powers as circumstances require.

Importantly, it is expected that the decision-making requirements in a technical assistance notice will require consultation with a provider before issue in the vast majority of cases. An agency head will likely not be able to be satisfied of the technical feasibility of a notice, or the legitimate interests of a provider (see proposed section 317RA), without first discussing the possible terms of a notice and its impacts on a provider’s operations.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/011*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q2) - Address the problem of encrypted communications.

Asked:

2. The United Nations Special Rapporteur on the right to privacy has recommended alternative collaborative pathways with industry to address the problem of encrypted communications for law enforcement and intelligence activities.
a. Prior to developing the current bill were other alternatives considered?
b. Why were those alternatives not pursued?

Answer:

a. Prior to developing the current bill were other alternatives considered?

Yes. The Department considered a number of legislative and non-legislative options before commencing drafting on the legislation. These alternatives included requiring exceptional access solutions, at both the hardware and software levels, to enable law enforcement to receive content in the clear, even in cases where it would be end-to-end encrypted.

Purely voluntary industry co-operation schemes were also considered.

b. Why were those alternatives not pursued?

Some of these alternatives are being pursued. To respond to the complications caused by encryption Australia is adopting a holistic approach that avoids weakening encryption, as recommended by the United Nations Special Rapporteur.1

The Australian Government is heavily involved in collaborative industry forums, like the Global Internet Forum to Counter Terrorism mentioned by the Special Rapporteur.2 Senior representatives from the Australian Government attended the Global Internet Forum to Counter Terrorism in 2017 to discuss issues like countering

[1] *Submission 81*, p. 15
[2] *Submission 81*, p. 15

violent extremism and encryption with key industry stakeholders. The Australian Government continues to engage with industry on security matters in a wide range of domestic and international fora.

Legislative solutions that would mandate a specific form of exceptional access were not pursued given the legitimate concern that such approaches could fundamentally weaken the security of third-party devices and services. Absent the more draconian requirement of set exceptional access solutions, the Department opted for broader framework of industry cooperation that would enable law enforcement and providers to reach mutually agreeable outcomes without undermining cybersecurity. The technological neutrality of the framework and its global protections enable agencies to approach industry with a problem and work together to achieve access solutions that leverage the interests and expertise of industry.

The Department fully recognises that this approach has its limitations and some services, particularly end-to-end encrypted services will remain a problem for evidence and intelligence collection. However, the flexible nature of the framework will allow agencies to overcome some of the challenges associated with these services by enhancing indigenous capabilities.

This industry assistance regime is just one part of this holistic approach. The Bill's other schedules are designed in compliment and are intended to addresses the problem of encryption without requiring a 'backdoor'. Alternative collection methods in the independently authorised covert and overt computer access warrants (Schedules 2, 3 and 4) will enable agencies to access data at end-points where it is not encrypted without compromising broader services or devices or even the encryption itself. Increased penalties for non-compliance with orders by judicial officers for access to a phone will incentivise the users and administrators of relevant device to cooperate with overt and warranted agency searches.

While the Department appreciates the voluntary assistance providers already give to agencies, it was determined that purely voluntary schemes would not be as effective as necessary. Many providers desire, or require, an obligation to assist and firmer legal footing for cooperation. From a social licence perspective, the providers in the Australian market should recognise that operating in this market carries an expectation that they assist law enforcement and security authorities when their products are being used for illicit activity.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/012*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q3) - Capacity to unlock encrypted communications

Asked:

3. The United Nations Special Rapporteur on the right to privacy has questioned whether government agencies already have the capacity to unlock encrypted communications.2 Could the Department please respond to this evidence?
a. The agencies have reported that 90 per cent of communications intercepted are encrypted. Of those communications, what impact (in terms of duration) is the attempted decryption having on current investigations and prosecutions?
b. Has a criminal prosecution failed because of a lack of evidence that would otherwise have been able to be provided if encrypted communications were either a) able to be accessed or b) accessed within a shorter period of time?

Answer:

a. The agencies have reported that 90 per cent of communications intercepted are encrypted. Of those communications, what impact (in terms of duration) is the attempted decryption having on current investigations and prosecutions?

As the Australian Federal Police has stated, approximately 90 per cent of the data it intercepts pursuant to a telecommunications warrant issued by a Judge or Administrative Appeals Tribunal member is now encrypted. The Australian Federal Police does not have a means of decrypting this collected product. Rather the Australian Federal Police must seek alternative means of locating and accessing these communications at their start or end point. This includes applying for and deploying physical and technical surveillance, the use of undercover operatives and human sources, the application of a mutual assistance request where it is identified that this material is accessible from a third party located in a foreign country, or the execution of a search warrant to locate and seize the device from which the message was sent or received. This creates an additional resource burden on law enforcement agencies, diverting resources from other activities. These alternative activities may pose significantly higher personal risk to the safety of officers.

A number of factors make it challenging to exercise these alternative methods, for example, the speed and ease with which electronic communications are deleted, and the difficulty of locating and seizing devices. As a result, the majority of encrypted

communications that the Australian Federal Police is lawfully permitted to access are never subsequently located or recovered through alternative means.

b. Has a criminal prosecution failed because of a lack of evidence that would otherwise have been able to be provided if encrypted communications were either a) able to be accessed or b) accessed within a shorter period of time?

The *Prosecution Policy of the Commonwealth* provides that before a prosecution can be commenced, the Commonwealth Director of Public Prosecutions must be satisfied that there is sufficient evidence to prosecute the case. Where there is a lack of evidence in a criminal matter, whether because of encrypted communications or otherwise, the Australian Federal Police does not lay charges.

As per the response to question 3a, as the majority of encrypted intercepted content is never successfully accessed, it is impossible to say what potential evidence was contained within these communications that would have allowed a prosecution to progress where insufficient evidence otherwise existed.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/013*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q4) - Designated communications provider

Asked:

4. Of the current assistance that is being provided by companies that fall within the definition of a designated communications provider (DCP), in what countries are these companies predominantly legally based?a. For a company that is based completely outside of Australia's jurisdiction, such as Facebook with no legal presence in Australia, how will Australia seek to enforce the Bill's compliance obligations in Division 5?

Answer:

Carriers and carriage service providers are identified in items 2 and 3 of the table of designated communications provider in section 317C. Currently, industry assistance is overwhelmingly provided by these entities. This is due to a few factors; the traditional dominance they have in the Australian communications market, the fact that these services form the backbone of the telecommunications system and, importantly, the existing regulatory regimes that apply to them. For example, section 313 of the *Telecommunications Act 1997* places a standing obligation on these entities to provide reasonably necessary assistance to authorities of the Commonwealth, State and Territory. This obligation serves as a formal basis for cooperation between agencies, carriers and carriage service providers and establishes a regulatory framework to facilitate assistance.

Outside of the *Telecommunications Act 1997* there are no substantial regulatory frameworks that govern law enforcement and national security assistance from the communications industry; particularly not for designated communications providers who are not carriers or carriage service providers.

Regular, voluntary, assistance is also received from some of the bigger technology companies based in the United States. This mainly reflects the growing dominance of the over-the-top communications they provide, like instant messaging, and the proliferation of their products in the Australian market. As noted in the Department's original submission to the Committee, the communications industry has become increasingly globalised and the services and devices Australians use frequently operate without direct control by domestic carriers.[1]

a. For a company that is based completely outside of Australia's jurisdiction, such as Facebook with no legal presence in Australia, how will Australia seek to enforce the Bill's compliance obligations in Division 5?

Division 5 enables the Commonwealth to apply for a suite of orders that may be sought in the event of non-compliance with an industry assistance notice. Section 317ZL establishes a regime for offshore service of a summons or process to a proceeding under Schedule 1. If the body corporate was incorporated outside Australia and did not have a registered office within Australia, but conducts activities within Australia, then the notice could be served at the address where the activities are conducted. Similarly, a summons or process could be served on the provider's agent in Australia. The *Acts Interpretation Act 1901* and the *Telecommunications Act 1997* each establish additional avenues for service that could apply in these circumstances.

If an offshore designated communications provider failed to comply with these orders or attend a summons, the Federal Court may pursue a range of options to seek enforcement and has significant powers to punish for contempt (this includes powers to fine, imprison or order sequestration of assets). The *Federal Court Act 1976* and the *Federal Court Rules 2011* detail the range of enforcement options and procedures available to the Court. The relevant jurisdiction is Australia and it may be open to the Federal Court to consider enforcement actions against corporate assets or activities in Australia.

Australia has arrangements in place with a number of countries for the reciprocal enforcement of judgments, including the enforcement overseas of judgments of Australian courts.[2] In certain circumstances, these arrangements would enable an overseas court to enforce judgments imposed by an Australian court.

The Bill reflects the principle that the broader entities who benefit from their interaction in the Australian market have an obligation to assist authorities to resolve legitimate public safety concerns. While enforcement is subject to jurisdictional challenges, the Bill's mechanisms and powers available to the Federal Court allow the Government to comprehensively pursue compliance where tangible aspects of a body corporate are within Australia's borders.

[1] Submission 18, pp. 12-13
[2] See for example the *Foreign Judgments Act 1991* the *Foreign Judgments Regulations 1992*.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/014*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Impact on business and global competitiveness (Q5) - Impact on businesses

Asked:

5. A number of submitters have expressed concern about the impact on businesses, particularly small businesses, when complying with industry assistance measures.3
a. Has the Government prepared a regulatory impact statement on the Bill?
b. If so, please provide a copy to the Committee for its consideration.
c. If not, and noting that all Cabinet submissions require at RIS,4 what are the reasons for not developing a regulatory impact statement on the Bill? Outside of a RIS, what work, if any, has the Department undertaken to assess the impact to business? What was the outcome of that work?

Answer:

a. Yes. The Government prepared a short form regulatory impact statement.

The regulatory impact of the industry assistance measures will be minimal.

The measures themselves are not standing obligations and will be largely issued in response to ad-hoc investigative needs. Where capabilities are developed, this will be targeted and not against a ‘class’ of designated service provider.

Further, the default basis of cost-recovery is no-profit / no-loss and, as such, the resourcing impost on industry is expected to be neutral. While the Bill does allow for the Government not to provide full compensation for assistance, this option may only be exercised in the public interest and is subject to high statutory thresholds. It is expected to be exceedingly rare and only in cases where a provider has been negligent or wilfully contributed to poor law enforcement and security outcomes.

The clear expectation, supported by the legal threshold, is that requirements set in a notice will be proportionate to the seriousness of the investigation and take into consideration the legitimate interests of the designated communications provider to whom the notice relates – as set out in section 317RA.

b. The Department will provide a copy to the Committee.
c. A short form regulatory impact statement was prepared.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/015*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 - Scope - Types of assistance—'listed acts or things' (s 317E) and 'listed help' (s 317T (4)) - (Q6) - System design

Asked:

6. For the public record, could a notice or request be issued by the relevant decision-maker that would require a designated communications provider to design their system for exceptional access by law enforcement or intelligence agencies?

Answer:

No. Technical capability notices could not be used to require exceptional access solutions.

As many submitters have noted they are not aware of any system of exceptional access that would not undermine encryption or create so-called 'back doors'. Proposed section 317ZG prohibits the construction of implementation of systemic weaknesses, the ordinary meaning of which generally refers to a weakness in one part of the system which would compromise other parts of the system or the system itself, rather than just a particular part. Most exceptional access solutions require deployed system wide changes that add an additional point of access for authorities, the effect of which may create another vector for malicious attack. While the cyber security implications of a technical capability notices need to be contemplated in each circumstance, the Department considers that there are significant risks that such changes may create a material weakness that compromise the whole system and thus attract the prohibition. To remove doubt, prosed subsection 317ZG(2) notes that prohibitions includes any requirements that would render systems of encryption or authentication, the crucial security measures in devices and services, less effective. In sum, the technical capability notices would have to provide exceptional access for law enforcement without jeopardising the security of users. Only a perfect exceptional access system, one which provides law enforcement access to a targeted user without materially weakening the security of non-target users, would be permissible under the language of the Bill, and such a system does not exist, nor is it likely to ever exist.

Aside from the prohibitions in proposed section 317ZG, an exceptional access solution would need to meet the standards of reasonableness, proportionality, practicality and technical feasibility to the Attorney-General's satisfaction. Given that such solutions typically require fundamental, system-wide designs, the thresholds for satisfaction will be very high and the competing interests of law enforcement, security, industry interests, privacy and cybersecurity will need to be weighed carefully.

The Bill does not explicitly rule-out exceptional access solutions, as they are many and varied. It is not practicable to explicitly prohibit each in the legislative text. Instead, the Department has created a prohibition that reflects core principles of cyber security and robust decision-making criteria that can be applied against each proposed solution. The combined effect of these measures is to make any of commonly referenced exceptional access solutions infeasible.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/019*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 - Industry Assistance - Structure (Q10) - Encrypted platforms

Asked:

10. For encrypted platforms, is metadata of those communications also encrypted?

Answer:

Most over-the-top communications platforms that provide encrypted messaging services also encrypt the metadata attached to those communications. Some platforms may provide sufficient metadata to identify the application being used (e.g. WhatsApp) and the server it is connecting to (including the date, time and data size) but often multiple layers of encryption are used meaning that there is no way of distinguish between an encrypted communications platform and an encrypted webpage. Where the application is identified it can be difficult (or impossible) to distinguish between data that is being sent and received from the device due to actions of the user, and data that is continuously and autonomously being sent by the server or device announcing it is online and ready to receive information.

This means that under intercept, agencies are often unable to determine the recipient of an encrypted conversation. To establish an encrypted communication channel, however, limited metadata (i.e. IP address of platform provider or recipient) must be unencrypted.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/020*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1—Industry Assistance - Structure (Q11) - Industry assistance measure

Asked:

11. Other than an update that was designed to rectify a systemic weakness or vulnerability in a form of electronic protection (as provided in the limitation s 317ZG(1)(b), could an industry assistance measure be issued that would request or compel a DCP to delay or otherwise prevent a system update?

Answer:

In the language of the Bill, technical assistance notices and technical capability notices cannot do anything that makes a form of electronic protection less effective than it would otherwise be. If the update does address another security vulnerability in the system – other than a systemic weakness or vulnerability – delaying this update would make the electronic protection less effective and be impermissible.

If the update in question does not improve the security of the system and only pertains to another feature of the system, this may be permissible. However, the Department notes that it would be extremely difficult to justify a delay on a system update of an entire service to the standards of reasonableness and proportionality and any such decision would be open to challenge in judicial review.

Such an action is analogous to the disruption of services through section 313 of the Telecommunications Act. As the *Guidelines for the use of section 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services* make clear, these actions are not taken lightly within agencies and a number of strict internal considerations are met before the disruption activity occurs. Section 313 does not contain the significant limitations and robust decision-making criteria of the proposed industry assistance measures, which will also be supported by existing internal procedures.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/021*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1—Industry Assistance - Structure (12) - Legislative instrument

Asked:

12. The Minister may, by legislative instrument, determine that more kinds of acts or things be included in the definition of 'listed help'.8 For clarity, would this legislative instrument be made public once determined by the Minister?

Answer:

Yes. A determination under section 317T(5) is a legislative instrument and will be tabled in Parliament.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/022*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Limitations - Systemic weakness / vulnerability (Q13) - Understanding of this term

Asked:

13. In the absence of specific legislative definition, the terms ‘systemic weakness’ and ‘systemic vulnerability’ will take their ordinary meaning. If a court were asked to adjudicate on the scope of either term, what existing legislation or case law would guide a court’s understanding of this term?

Answer:

The term ‘systemic weakness’ would be construed in accordance with the natural and ordinary meaning. The ordinary meaning of the term ‘system’ encompasses interacting or interdependent items that form a unified whole, and the ordinary meaning of the term ‘systemic’ is ‘relating to a system’ rather than a particular part. Taken together, the Department submits that these terms generally refer to a weakness or vulnerability in one part of the system which would compromise other parts of the system or the system itself, rather than just a particular part.

If the ordinary meaning of the terms results in ambiguity, or leads to a result that is manifestly absurd or is unreasonable, the Court may rely on extrinsic material such as the explanatory memorandum. The explanatory memorandum to the Bill explains that the intent of section 317ZG is to protect the fundamental security of software and devices.

Due to the technologically diverse and complex environment which these terms will be considered in, if a court were to consider these terms, it would consider them consistent with the rules of statutory interpretation, on a case-by-case basis, taking into account the circumstances of an individual matter.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/024*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 - Limitations - Systemic weakness / vulnerability (Q15) - Non systemic weakness

Asked:

15. The Office of the Victorian Information Commissioner described how a non-systemic weakness at first instance could become a systemic weakness when deployed later. Could the Department respond to this evidence?

Answer:

The Explanatory Memorandum to proposed section 317ZG distinguishes between capabilities deployed into a system and intended to remain there persistently with capabilities developed and held in reserve for use against specific targeted devices or systems.

The Office of the Victorian Information Commissioner's evidence challenges this distinction by proposing a scenario in which custom firmware developed to service a single request is used as the basis to respond to future requests. The ability to configure the capability initially developed, the Office of the Victorian Information Commissioner claims, to furnish later requests represents a systemic weakness. Further, the Office of the Victorian Information Commissioner claims that such a capability cannot be adequately secured to prevent it being used by malicious actors.

The Department disagrees with these claims by the Office of the Victorian Information Commissioner. Custom firmware built to address one notice or request is not a systemic weakness unless it is deployed to users other than the targeted user. So long as the capability is held in reserve it does not jeopardise the security of other users and is not a systemic weakness.

The Department refers to its answer to question 7 above as the hypothetical is analogous.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/025*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Limitations - Systemic weakness / vulnerability (Q16) - TARs -

Asked:

16. Why has the limitation not been extended to TARs?

Answer:

The Department is not sure what limitation is being referred to. In general terms, technical assistance requests have been designed more flexibility than the coercive powers in Schedule 1. Their voluntary nature and the clear requirement of agencies to inform providers of their voluntary nature (see section 317HAA) enables a provider to easily disregard a request.

As *Australia's Cyber Security Strategy* 2016 sets out, the Australian Government has a strong commitment to cyber security. Agencies do not have an interest in jeopardising the communications security of ordinary Australians and requests under technical assistance requests will be consistent with this principle and the legitimate functions of Australian's key law enforcement and intelligence agencies as prescribed by law.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

() – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Limitations - Systemic weakness / vulnerability (Q17) - OAIC recommendation

Asked:

17. The OAIC has recommended an amendment that would introduce a defence of reasonable belief of a systemic weakness/vulnerability (section 317ZG) to the offences in Division 5.11 Could the Department please respond to this recommendation?

Answer:

Proposed new Division 5 of Part 15 of the Telecommunications Act does not include any new offence provisions for non-compliance. It includes various enforcement provisions including civil penalties, enforceable undertakings, and injunctions. The concept of a 'defence' is unusual in relation to enforceable undertakings and injunctions, although honest and reasonable mistake of fact is available.

A further/new statutory defence to the civil penalty provisions at sections 317ZA and 317ZB would create a new avenue by which a carrier, carriage service provider or designated communications provider (a provider) can claim that they are not required to comply with a requirement under a notice. Other than the defence in proposed section 317ZB, the current avenue in the Bill for a provider to claim that they are not required to comply with a requirement under a notice is to challenge the validity of the notice through judicial review.

Through judicial review of the decision to issue a notice, a court would consider whether the notice was given following all statutory requirements and administrative law requirements, including that the required state of satisfaction of the decision maker existed at the time of the decision to issue the notice.

In addition to judicial review, section 317W of the Bill already contains a mechanism to ensure that satisfaction is reached for a technical capability notice: a communications provider may make submissions and an independent assessment may be made about whether the capability notice would contravene section 317ZG. A "reasonable belief" defence is therefore not necessary and would be difficult to make out where the parties have obtained an independent expert report which concludes that the capability notice does not contravene section 317ZG.

In comparison, in a civil penalty proceeding where the provider is claiming a defence of reasonable belief of a systemic weakness/vulnerability held by the provider, a court will be considering the existence of that reasonable belief held by the provider rather than considering any actions or state of mind of the decision maker who issued the notice.

The outcome of both processes is the same - that is, if the argument made by the provider is successful before the court then they are not required to comply with the notice. One process is analysing the administrative decision making process, and the other is only considering the reasonable belief of the provider.

Given that a technical assistance notice cannot require the construction of new capabilities and assistance will be consistent with the existing functions of a provider, there is no need for a section 317W process (the risk of systemic weaknesses is significantly lower). Further, the robust decision-making requirements likely make consultation necessary in the vast majority of technical assistance notice cases.

Given the multiple avenues to determine and challenge the fact that a systemic weakness may be a risk of technical capability notice requirements, the Department does not believe a new defence is necessary.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/027*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 General limits re warrants (Q18) - 317ZH not been extended to TARs

Asked:

18. Why has the limitation at 317ZH not been extended to TARs?

Answer:

a. The limitation at section 317ZH is designed to prevent law enforcement agencies gaining the ability to force compliance in areas where a judicially authorised warrant is currently required by law. Technical assistance requests have been excluded from this limitation because they are a voluntary mechanism. This voluntary nature has two relevant implications.

Firstly, where evidence can be obtained from a target willing to cooperate freely with law enforcement, a warrant is not required. Where a provider is willing to cooperate with a technical assistance request they should be allowed to do so regardless of whether a warrant would be required if they were unwilling to cooperate.

Secondly, the voluntary nature of technical assistance requests means that anything they request may be freely refused by the provider. Where a provider is unwilling to cooperate in an area where a warrant is needed to oblige compliance, in no way will the receipt of a technical assistance request compel the provider to cooperate with law enforcement. Technical assistance requests, therefore, are inherently limited in the manner prescribed by section 317ZH.

A technical assistance request does not enable an agency to compel a provider to undertake illegal activity or enable an agency to undertake illegal activity itself. Warrants are generally an instrument to authorise otherwise prohibited conduct.

Further, technical assistance requests would not be in any way further limited if they were included within the limitation of 317ZH as, per the wording of the section, a technical assistance request would have “no effect to the extent (if any) to which it would require a designated communications provider to do an act or thing…” As technical assistance requests are a voluntary mechanism, they can never require providers to do an act or thing. As such, the limitation as drafted would not apply to technical assistance requests.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/028*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 General limits re warrants (Q19) - Giving effect to a warrant.

Asked:

Subsections 317ZH(4) and (5) uses the terms 'giving effect to a warrant'. What does the term mean?

Answer:

a. The term 'giving effect to a warrant' reflects the function of a technical assistance notice or a technical capability notice to require a provider execute the relevant underlying warrant. Analogous provisions are in paragraphs 313(7)(b) and 313(7)(d) of the *Telecommunications Act 1997* which include in the notion of 'giving help', the act of giving effect to a stored communications warrant or an authorisation for telecommunications data under the *Telecommunications (Interception and Access) Act 1979*. The intent is to create an obligation to effect a valid warrant. It is not intended to replace the warrant or extend the inherent limitations (including jurisdictional limitations) within a warrant itself. The base and active warrant is still required.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/029*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Specific questions on TCNs (Q20) - Why are TANs required

Asked:

As proposed, a TCN may require a DCP to (1) develop a new capability or (2) provide assistance that the provider is already capable of providing. The Bill employs identical language for this second option as is employed for TANs. Some submitters have questioned the need for TANs in light of the second option.
a. Why are TANs required if a TCN could be issued that required a DCP to provide assistance that it is already capable of providing?

Answer:

a. A technical assistance notice is intended to support dynamic and continuous relationships between agencies and providers. It is purposively flexible to ensure that critical assistance can be achieved in a timely manner and that agencies and providers can have direct conversations about what assistance is feasible in the circumstances and how best industry can help. It is limited to help that a provider is already capable of giving, that is, the things for which it has the ability to do due to its existing business functions.

In contrast, a technical capability notice must be issued by the Attorney-General and is subject to significant mandatory consultation periods. The reason for the higher threshold lies in the fact that the notice can require the construction of capabilities that are ancillary to business requirements and go beyond a provider's ordinary needs. While a technical capability notice may also require a provider to do things they are currently capable of doing, this was inserted to remove the need for an additional technical assistance notice to be issued to allow use of a capability developed under the higher threshold technical capability notice.

To ensure that the measures create a productive and responsive framework for industry assistance, the graduated approach embodied by agency issuance of technical assistance notices is necessary. This also recognises the fact that multiple Australian jurisdictions are included within the regime, each with their own direct relationships with providers. Inserting the Attorney-General at this stage would impede the proper working of the regime and act as a disproportionate check on ongoing and targeted assistance from providers.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/031*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Specific questions on TCNs (Q22) - Offensive capability

Asked:

22. Could a TAR, TAN or TCN be issued to develop an offensive capability, for example in cyber-warfare? Please provide separate answers on the different types of notices that can be issued.

Answer:

Offensive cyber capabilities are within the remit of the Australian Signals Directorate.

Under the proposed legislation, Australian Signals Directorate would be able to issue a technical assistance request in relation to the proper performance of its functions. These functions include providing assistance to the Defence Force in support of military operations, which extends to providing offensive cyber support. For example, the legislation would allow Australian Signals Directorate to seek technical advice from a designated communications provider to understand a certain technology. The information might subsequently be used to develop offensive cyber tools to support military operations overseas. These operations themselves are subject to stringent legal oversight and are consistent with Australia's obligations under international law.

Designated communications providers would co-operate with such requests on a voluntary basis.

The Australian Signals Directorate could not rely on a technical assistance request to ask a designated communications provider to conduct the offensive cyber operation itself.

There is no proposal for the Australian Signals Directorate to be able to issue technical assistance notices or technical capability notices.

Australian Signals Directorate could not rely on a technical assistance request to ask a designated communications provider to conduct the offensive cyber operation itself.

There is no proposal for Australian Signals Directorate to be able to issue technical assistance notices or technical capability notices.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/032*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Definition of DCP (Q23) - Class of designated communication's providers.

Asked:

23. Could a TAR, a TAN or a TCN be issued to a 'class' of designated communication's providers?
a. If so, what is the policy rationale for this approach?
b. If so, and with specific reference to a 'class'-based TCN, how would the consultation requirements be satisfied? Would agencies engage with the full class of providers at once? How would a 'technical expert' be assigned?
c. How would the secrecy provisions apply to the class of DCPs?

Answer:

No. The industry assistance regime is directed towards securing assistance from singular providers.

a. N/A

b. N/A

c. N/A

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/033*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1— Industry Assistance - Structure (Q24) - Concerns on designated communications

Asked:

24. A number of stakeholders have expressed concern about the inclusion of componentmanufacturers in the definition of a 'designated communications' provider. What is the reason for including component manufacturers in the definition? What problem has been presented in practice that would explain to the public the reason for its inclusion?

Answer:

a. The definition of designated communication provider has been drawn to encompass the entire supply chain of technology and communication device manufacturers. This is because it is unclear at which point in the supply chain intervention will be necessary to facilitate law enforcement's access. It may be necessary in certain situations to intervene at the level of a component manufacturer in order to provide a pathway for lawful access while avoiding placing the integrity of other security features in jeopardy. An isolated hardware fix would be especially effective to avoid the generation of systemic weaknesses as it would be physically limited to the targeted components in the targeted device.

Future system designs and software capabilities are unknowable in such a technologically complex and evolving industry and it is important that the Bill operate flexibly and provide parties with a sufficient range of possible methods for access without create artificial restrictions.

The concern that the inclusion of component manufactures will compromise supply chains is unfounded. The ability of the measures to introduce changes at the hardware level across a product line is out of scope. Not only do the key decision-making criteria of reasonableness, proportionality, practicality and technical feasibility apply but the prohibition against systemic weaknesses is clearly limiting against any requirements to compromise components in non-target devices.

Additionally, if component manufacturers are exempted from the definition of designated communication providers, bad actors will be encouraged to use this carve-out as a refuge from the broader operation of the Bill – potentially relying upon

hardware-based verification or encryption methods that will then be beyond the scope of the law to regulate. Limiting the Bill's ability to intervene at any point of the supply chain can potentially create loopholes that will be abused. As stated in previous submissions, the scope of the law, bounded by reasonableness and security limitations, enables agencies to secure targeted assistance where it is most needed. The alternative approach is to mandate set exceptional access methods which, as many submitters note, carry serious concerns for cyber security.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/034*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Issuing the notice or request - Authorisation (Q25) - Judicial authorisation

Asked:

25. A large number of stakeholders have expressed concern that industry assistance measures should be issued by a judicial officer, wish some noting that judicial authorisation and ministerial authorisation are required under the United Kingdom's Investigatory Powers Act 2016.17 Why is judicial authorisation considered inappropriate for Australia's equivalent scheme?

Answer:

a. The Department disagrees with the characterisation that the Bill represents a scheme equivalent to the UK's *Investigatory Powers Act 2016*. From the Department's previous answers to Questions on Notice from the Parliamentary Joint Committee on Intelligence Security of 23 October 2018:

> "While there are parallels between the intent of aspects of the *Investigatory Powers Act 2016* (UK) 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 *Investigatory Powers Act 2016* (UK), 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 *Investigatory Powers Act 2016* (UK) 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* regulates targeted interception powers and data retention, and the *Surveillance Devices Act 2004* 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 *Investigatory Powers Act 2016* (UK) and this Bill, and the significant differences in the available scope of a technical capability notice, the 'double-lock' regime (judicial and Ministerial authorisation) in the UK IPA is not appropriate for this Bill. The powers in the *Investigatory Powers Act 2016* (UK) are more expansive and may have more significant impacts on providers than the proposed powers in Schedule 1."

Further, judicial authorisations for technical capability notices under the *Investigatory Powers Act 2016* (UK) are a consistent feature of the entire Act's authorisation process. The judicial commissioner role and the functions of the Investigatory Powers Commission have been tailored to support the warrant powers under the Act – they are not in place solely to guide and decide on technical capability notices. Australia already has a regime of judicial oversight that applies to powers that Schedule 1 of the Bill is designed to support.

Ministerial authorisations are a feature of the Australian legislative landscape. From the Department's previous answers to Questions on Notice from the Parliamentary Joint Committee on Intelligence Security of 23 October 2018:

> "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 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* is an example of an existing regime that requires a Minister to make a decision based on their judgement of complex technical issues. The *Security of Critical Infrastructure Act 2018* 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 technical capability notices 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 *Security of Critical Infrastructure Act 2018* 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 *Security of Critical Infrastructure Act 2018* may be based on an increase or creation of systemic weaknesses or vulnerabilities.
>
> Similarly, section 315B of the *Telecommunications Act 1997* 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."

Judicial authorisation is further inappropriate for the powers contained in Schedule 1 of the Bill as they do not relate to the actual viewing of communications content or the actual collection of evidence. These powers solely provide law enforcement with assistance to gather evidence where it would otherwise be inaccessible for technical reasons. Any actual evidence gathering requires a warrant of the relevant kind which will involve seeking judicial authorisation.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/035*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 — Industry Assistance - Structure (Q26) - Exercise of powers

Asked:

26. Could the independence of a statutory oversight body (such as the Law Enforcement Conduct Commission in NSW) be compromised by requiring approval of the exercise of one of its powers by the federal Attorney-General? Are there analogous powers that an independent statutory body exercises with the approval of a member of the Executive?

Answer:

a. As first law officer of Australia the Attorney-General is responsible for protecting and promoting the rule of law. Recent machinery of Government changes moved significant oversight bodies and functions into the Attorney-General's portfolio, creating a clear mandate for integrity in the office. Further, the Commonwealth Attorney-General is sufficiently removed from State and Territory statutory bodies to make the risk of compromise a remote one.

While the Department is not aware of an analogous situation affecting the powers of independent statutory authorities, this is nonetheless a justified requirement of technical capability notices. The Attorney-General as appointed first law officer of Australia by the Governor-General is the appropriate officer to oversee the exercise of these powers and is sensitive to maintain the independence of statutorily independent bodies. The Attorney-General has routine knowledge of sensitive capabilities as the approver of Australian Security Intelligence Organisation warrants and is well-placed to decide on how they should be developed and utilised to their maximum effect across the Commonwealth, State and Territories.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/037*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Relevant objective (Q28) - National security

Asked:

28. The relevant objective for all notices and requests refers to the term 'national security'. How will the term be defined?

Answer:

The phrase "national security" takes its ordinary meaning. We note that it is used in a variety of ways in the Bill including as part of the broader phrase 'in the interests of Australia's national security, Australia's foreign relations or Australia's economic well-being". This broader phrase is used in the *Intelligence Services Act 2001*, *Telecommunications (Interception and Access) Act 1979* and the *Australian Security Intelligence Organisation Act 1979* in relation to the collection of foreign intelligence.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/039*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Reasonable and proportionate & technically feasible (Q30) - TAN or TCN criteria

Asked:

30. The relevant decision-maker must be satisfied that a TAN or TCN is reasonable and proportionate. Why has this criteria not been extended to a decision-maker issuing a TAR?

Answer:

a. Technical assistance requests are voluntary instruments and were an unreasonable or disproportionate technical assistance request issued to a provider they would freely be able to refuse anything it requested.

Technical assistance requests represent a codification of a present, informal arrangement between law enforcement and some providers. Presently, some providers will offer assistance to law enforcement on a voluntary basis when asked to do so. Implicit in this arrangement is that providers are not asked to behave unreasonably or offer assistance disproportionate to the crime being investigated as the assistance would otherwise not be forthcoming.

The lower thresholds for issuing a technical assistance request are then recognition of the reality of how assistance is sought and proffered currently. The less intrusive nature of the instrument is also designed to avoid overburdening decision-makers through codification and thereby creating a less effective mechanism than the informal process which presently exists.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/040*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Reasonable and proportionate & technically feasible (Q31) - Two standards

Asked:

31. Stakeholders have expressed concerns that the bill would only require a subjective standard to be satisfied for the questions of reasonable proportionate and technically feasible and have recommended an objective standard be required (for example, Apple, pg 5). What would be the implications of such an approach? Please provide analogies to other areas of Australian law and examples of how the two standards (objective and subjective) could apply in practice.

Answer:

a. The Department noted the rationale behind a subjective standard in its original submission.[1] Section 313 of the *Telecommunications Act 1997* establishes an objective standard for industry assistance. The objective standard has led to undue ambiguity as the scope of what constitutes 'reasonably necessary' help is undefined and cannot be settled by a deciding party. This is particularly problematic as the section does not clearly set out what type of assistance may be required. This 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. For example, 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.

The lack of clearly defined obligations, as a consequence of the objective standard, has also meant that critical assistance sought under the authority of section 313 has been neglected in favour of more explicit requirements like the maintenance of traditional interception capabilities. Ambiguity introduces delays into the assistance process as providers (understandably) want to be clear on the legality of the help they provide. The Department expects similar problems if an objective standard was to be applied to the current regime.

[1] *Submission 18*, p. 29

The Department suggests that industry expertise rests in commercial operations and technical competency – it does not extend to evaluating the threat environment and determining the necessity of agency actions. These are proficiencies held by senior decision-makers within agency and national security ministers such as the Attorney-General.

The subjective nature of the decision making requires the decision-maker to actually be satisfied that the requirements imposed by a notice are reasonable and proportionate and that compliance with the notice is practicable and technically feasible. Case law notes that this satisfaction must be informed on the correct understanding of the law – decision-makers cannot take into account matters which would be extraneous to any objects the legislature could have had in view.[2] This is not unbounded discretion - if, for example, a designated communications provider provided clear and timely information that requirements in a notice were not technically feasible or the impact of the notice was unduly severe and the decision-maker ignored those concerns, a cogent case could be made in review that the decision-maker did not in fact reach the requisite state of mind. In practice, this would mean that a decision-maker would need to consult with the designated communications provider about matters such as reasonableness, proportionality and technical feasibility before properly being reasonably satisfied that the request can be made.

[2] *Minister for Immigration and Multicultural Affairs v Eshetu* (1999) 193 CLR 611 at 651-654; *Water Conservation and Irrigation Commission (NSW) v Browning* (1947) 74 CLR 492 at 505.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/042*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 Manner and form (Q33) - Information to be included in the notice

Asked:

33. The Bill does not outline the form by which a TAR, TAN or a TCN, for example what information must be included in the notice (other than, for a TAR that compliance is voluntary, and for TANs and TCNs, the compliance and enforcement provisions of the Bill).
a. What minimum information will these notices include?

Answer:

a. Except in emergency circumstances a request or notice must be in writing. Within 48 hours of issue, all notices must be in the form of a written record.

The specific aspects of the form is an administrative matter best dealt through guidelines and centrally administered documents. The Department will support standardisation amongst requests and notices.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/043*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q34) - Appointment of technical expert.

Asked:

34. The Bill provides for the appointment of a technical expert to prepare a report on the question of whether the notice contravenes the systemic weakness/vulnerability limitation. Under what process will these experts be appointed? Will these appointments be publicly known?

Answer:

a. The process as set out in the legislation enables joint appointment of a technical expert by the Attorney-General and the relevant provider. The key element to this process is mutual agreement – the expert must be mutually agreeable to both main parties involved in the issuance of technical capability notice. Subsection 317W(8) requires that this person must have sufficient knowledge to assess whether the proposed notice would contravene the prohibition on systemic weaknesses or vulnerabilities.

Given the diversity of providers in the communications industry and the range of systems / capabilities that agencies may be dealing with, it was considered important that both parties retain the discretion to choose an expert with the most suitable experience in the circumstances. Given the sensitive nature of both agency and provider information appointment by agreement will ensure that each party has faith in the integrity of the expert and that the individual/s is sufficiently cleared to handle information which forms part of the assessment.

There is no requirement for the publication of appointments.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/044*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q35) - Appointment of cost negotiators.

Asked:

35. The Bill provides for the appointment of a costs negotiator where the DCP and decision-maker disagree on the profits/costs incurred from complying with the TAN/TCN, and the Minister may specify one or more persons as cost negotiators.
a. How will these persons be appointed? What process will occur prior to the Minister's decision? Will this list of persons be publicly known?

Answer:

a. Consistent with section 317ZK, the applicable costs negotiator is the Director-General of Security or the chief officer of an interception agency for a technical assistance notice. It is a person specified on the notice in the case of a technical capability notice. The cost negotiator, by default, negotiates costs with a provider. This does not occur just when there is disagreement. The Minister for Home Affairs does not have a formal role in appointing the cost negotiator.

The identity of the costs negotiator is public for technical assistance notices given their status as agency heads. The identity of the costs negotiator for technical capability notices would not normally be disclosed.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/045*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q36) - Consultation mechanism for TCNs (section 317W).

Asked:

36. Why was the consultation mechanism for TCNs (section 317W) not extended toTARs or TANs?

Answer:

a. The differing purpose and operation of technical assistance requests and technical capability notices, and technical assistance notices means that it is unnecessary to legislate consultation requirements for all powers in Schedule 1. Extending the consultation requirements also fails to consider the practical nature of Schedule 1 which is likely to be supported by informal consultation with designated communications providers throughout the development of requests or notices to ensure the requirements meet the objectives of agencies and do not adversely impact entities or the broader community.

Technical capability notices are supported by consultation requirements because of the gravity of these notices. The consultation framework under a technical capability notice establishes a formal period by which the Attorney-General can receive and consider technical information by designated communications providers, technical expert or other relevant party and factor this information into the ultimate form of requirements present in a notice. The intention of this framework is to ensure proportionate and mutually agreeable conditions can be set in a notice.

While technical capability notices are supported by strong limitations and safeguards, there is the potential that the requirements may have unintentional and disproportionate impacts on the designated communications provider. The legislated consultation period provides an opportunity for the designated communications provider to formally raise these issues, including whether the requirements systemically impacts the security of their networks and systems, which must be considered by the Attorney-General prior to the issuance of a notice. Given the gravity of these notices, it is important that the Attorney-General is supported by relevant information from the designated communications provider when determining the reasonableness and proportionality of a notice. This ensures that a technical

capability notice reflects the well-founded and legitimate issues and concerns raised by designated communications providers.

Technical assistance notices have a less significant impact as they can only be used to require designated communications providers to provide assistance that they are already capable of giving. Given the need for operational flexibility and the role of technical assistance notices in supporting ongoing relationships with providers, it is not desirable to establish a legislated consultation period. However, in most circumstances, it would be expected that an agency would need to consult with the designated communications provider prior to the decision-maker considering whether a notice is reasonable and proportionate. For example, noting technical nature of requirements, a decision-maker is unlikely to be satisfied of 'technical feasibility' without consulting with a designated communications provider beforehand.

The intention of technical assistance requests is to provide a legal basis for designated communications providers to provide voluntary assistance to agencies. As a result, non-compliance with the requirements of a technical assistance request will not attract any penalties. However, similar to technical assistance notices, it is likely that agencies will engage with designated communications providers to ensure that assistance can be sought on a voluntary basis. Technical assistance requests are also likely to be used relatively regularly to obtain minor or high-level information from designated communications providers. The Department sees no benefit in requiring mandatory consultation with designated communications providers when issuing a technical assistance request particularly as it may unintentionally create additional operational issues for agencies and impact the flexibility of requests.