QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/046*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q37) - DCP engagement to vary a TAN or TAR.

Asked:

37. Future Wise note that what is contained in the notice may not be what is the end product developed as a result of that notice. The bill does not require the notice to specify to any degree the type of work to be completed, nor provide a mechanism for the DCP to engage with the decision-maker to vary the notice once issued should the works be broader than originally envisaged in the notice. Should a DCP be able to engage with a decision-maker to vary a TAN or TAR (where consultation is not possible prior to issue) in such circumstances?

Answer:

Schedule 1 clearly sets out an ability to vary technical assistance requests (see section 317JA), technical assistance notices (see section 317Q) and technical capability notices (see 317X). The purpose of these variation powers is to ensure that providers and Government can implement requirements flexibility, according to the needs of both parties and account for unforeseen circumstances.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/049*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q40) - Greater transparency of new capabilities.

Asked:

40. A number of stakeholders have called for greater transparency of new capabilities developed under Schedule 1, with some seeking to compare the knowledge of existing telephone interception capability, with only the target/s of that interception not being publicly known.
a. Could you respond to the recommendations for any new capability to be publicly reported?
b. How is telephone interception capability (which is publicly known) different to the types of capability that will be developed under industry assistance measures (which will not be known)?

Answer:

a. The industry assistance framework allows for public reporting of technical capability notices through two mechanisms; (1) the mandatory annual reporting in section 317ZS and (2) the exception to unauthorised disclosure in subsection 317ZF(13) for statistical reporting on notices received. While these allow for the fact of a technical capability notice to be publically disclosed, they do not reveal the nature of the capability.

Publically detailing the specifics of a capability carries a significant risk that core law enforcement and security agency sources and methods will be revealed. This may alert persons under investigation of the fact and prompt them to further conceal their activities, frustrating and undermining investigations. In effect public disclosure enables criminal actors to evade legitimate detection and destroy evidence or intelligence.

Law enforcement experiences this phenomena frequently through capability discussion in court proceedings. Court processes and other legislation, like the *National Security Information (Criminal and Civil Proceedings) Act 2004* and the *Surveillance Devices Act 2004* (see section 47), recognise this phenomena and allow for the suppression of information (including information about capabilities) in Court.

To effectively do their jobs, agencies need to operate covertly and conduct operations in secret. These significant powers come with independent and ministerial oversight by dedicated and vetted bodies. This oversight not only goes to administrative compliance but propriety. Schedule 1 does not impede this oversight and exceptions to the unauthorised disclosure offences enable scrutiny of capabilities by the appropriate persons.

b. Interception is a broad, widely known and frequently utilised capability. It is explicitly regulated by the *Telecommunications (Interception and Access) Act 1979*. Likewise, the fact that agencies can undertake optical surveillance, use listening devices or track data is present on the face of legislation like the *Surveillance Devices Act 2004*. What is not publically known is the underlying capabilities that support these broader functions.

Warrants under both acts are executed and supported by a range of methodologies. It is the longstanding practice of the Australian Government not to discuss or reveal these methodologies (which are limited by publically scrutinised warranted powers).

A technical capability notice is flexibility designed to allow targeted, single capabilities to be developed and deployed and issued to a provider. This is distinct from interception or data retention capabilities that apply across a class of providers (carriers and carriage service providers). To publicise a capability is in effect signalling to persons who would seek to evade the law and conceal their activities how that could be achieved.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/050*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q41) - The Bill's interaction with the Public Interest Disclosure Act 2013.

Asked:

41. What is the Bill's interaction with the Public Interest Disclosure Act 2013?

Answer:

a. Public interest disclosures in relation to information obtained under this Bill is appropriately limited under the *Public Interest Disclosures Act 2013*, including by sections 33 and 41 which limit the operation of the Act in relation to conduct connected with intelligence agencies and intelligence information. The information obtained under this regime is likely to be of a sensitive law enforcement, national security and commercial nature, and may expose sensitive capabilities.

As a result, it is appropriate that legal restrictions apply to protect this information. The decision-making criteria, existing limitations on agency activities and oversight arrangements will ensure that the powers are exercised prudently and responsibly. The Inspector-General of Intelligence and Security has complaints and inquiries functions to which the Bill would be subject.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/051*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q42) - Commonwealth Ombudsman accessing TAR information.

Asked:

42. The Commonwealth Ombudsman has noted that his officers would be prevented from accessing 'TAR information', 'TAN information' and 'TCN information' as held by the agencies which the Ombudsman oversights.26 Why has the bill been drafted to exclude Ombudsman's legal access?

Answer:

a. Information that is subject to the unauthorised disclosure offence includes information about requests and notices. However, section 317ZF(3)(c) allows the disclosure of information in accordance with any requirement imposed by a law of the Commonwealth, a State or a Territory. The Ombudsman has extensive powers of inspection and their legal access is supported by requirements in Commonwealth law.

The Department considers that this exception allows the Ombudsman to conduct their existing oversight functions and scrutinise notices or requests made in support of an interception warrant or surveillance device.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/052*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q43) - OAIC and adverse impact on privacy.

Asked:

43. The bill expands the powers of agencies to obtain access to personal information. The OAIC notes that where there is an adverse impact on privacy, a commensurate increase in oversight, accountability and transparency is required.27 For the powers contained in Schedule 1, how are the oversight, accountability and transparency measures commensurate with the expanded powers?

Answer:

a. Schedule 1 does not expand the direct means by which agencies can obtain access to personal information. Consistent with section 317ZH and as currently the case, a warrant or authorisation will still be required to access personal information.

What Schedule 1 does is allow agencies to work closely with industry to ensure that underlying warrants can be effectively executed in a complex digital environment characterised by encryption.

Given that independently scrutinised or otherwise established evidence and intelligence collection methods remain the means by which agencies lawfully obtain data there is no need for, Schedule 1 to replicate the authorisation procedures of these powers. However, Schedule 1 does; (1) require additional decision-making criteria to guide orders for assistance that facilitate the execution of the underlying authority (privacy and cyber security are explicit considerations), (2) establish public reporting mechanisms, and (3) allow for independent oversight activities. Further, judicial review is available for providers who wish to challenge aspects of a notice.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/053*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q44) - Powers under Schedule 1

Asked:

44. The bill proposes to grant independent statutory oversight bodies with powers under Schedule 1, such as the Law Enforcement Conduct Commission in NSW. What oversight is provided by those agencies' use of the proposed powers in Schedule 1?

Answer:

Oversight bodies for each of the state and territory agencies with powers under the Bill, including independent statutory bodies, are listed in the table in question 45.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/054*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q45) - Oversight mechanisms.

Asked:

45. What oversight mechanisms would oversee the exercise of Schedule 1 powers by state police?

Answer:

a. The exercise of Schedule 1 powers by state police will be overseen by the oversight and anti-corruption bodies native to each state. As provided in the Department's previous answers to Questions on Notice from the PJCIS of 1 November 2018:

> "…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
Tasmania	**Tasmania Police**	Ombudsman Tasmania, Tasmania Integrity Commission

The Commonwealth Ombudsman may also have a role to play in overseeing state police investigations where those investigations have a federal element."

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/056*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q47) - Division 6 and DCP communication.

Asked:

47. Would the proposed sections in Division 6 in any way prevent a DCP from communicating its vulnerabilities to its customers?
a. If so, under what circumstances would a DCP be prevented from this communication?

Answer:

a. No. The provisions of Division 6 would not prevent a designated communications provider from merely communicating its vulnerabilities to its customers. Division 6 prohibits disclosure of technical assistance request, technical assistance notice and technical capability notice information, which are defined terms. That information relates to the giving, existence, variation, revocation or requirements of a notice/request, consultation on a notice, or things done in compliance with a notice/request.

The vulnerability would need to be so closely connected to the notice or request that disclosure would necessarily reveal technical assistance request, technical assistance notice and technical capability notice information as defined.
Further, the Bill does not allow a technical assistance notice or a technical capability notice to prevent a designated communications provider from rectifying systemic weaknesses or vulnerabilities (s317ZG). Rectification may require customers to be notified to update software and therefore necessarily be made aware of a vulnerability. The Bill envisages and allows that notification, even though it is potentially connected to a technical assistance notice or a technical capability notice.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/057*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q48) - Secrecy offences in Division 6. -

Asked:

48. What is the intention element for the secrecy offences in Division 6? Should unintentional disclosures be subject to a lower penalty?

Answer:

The offence of "unauthorised disclosure of information" in proposed subsection 317ZF(1) of the Bill includes (a) the physical element that a "person discloses information", in the circumstances that (b) the person is or was one of the persons provided in that paragraph, (c) the information is of the type provided, and (d)-(e) the information came into the person's knowledge or possession in one of the ways provided.

The offence in proposed subsection 317ZF(1) of the Bill does not specify the applicable fault elements. As a result, the relevant fault elements would be determined by reference to section 5.6 of the *Criminal Code Act 1995*.

The first element, that the person 'discloses information', is a physical element that consists only of conduct. Subsections 5.6(1) and 5.2(2) of the *Criminal Code Act 1995* would provide that, in order to prove this element, the person must have intended to disclose the information, meaning that he or she meant to engage in that conduct.

The remaining elements in paragraphs (a) to (e) of the proposed offence are physical elements which consist of a circumstance. Subsections 5.6(2) of the *Criminal Code Act 1995* would provide that the relevant fault element is recklessness, meaning that the person was aware of a substantial risk that the circumstance existed or would exist and, having regard to the circumstances known to him or her, it was unjustifiable to take the risk (see also subsection 5.4(1)). Subsection 5.4(4) of the *Criminal Code Act 1995* provides that, where recklessness is the fault element, proof of intention or knowledge would also satisfy that fault element.

A disclosure that is unintentional will not constitute an offence under proposed subsection 317ZF(1), therefore no penalty will apply. Further, proposed subsection 317ZF contains a range of exceptions to the offence where the disclosure is authorised.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/058*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q49) - the offence provision in 317ZA -

Asked:

49. The offence provision in 317ZA does not specifically include a knowledge requirement of the relevant notice.30 As a matter of legislative interpretation, how would the persons knowledge, or lack thereof, be considered by a court?

Answer:

Subsection 317ZA(1) requires carriers or carriage service providers to comply with a requirement under a technical assistance notice or technical capability notice to the extent that they are capable of doing so. Subsection 317ZA(2) prohibits persons from doing specific things which bring about a contravention of subsection 317ZA(1). Subsection 317ZA(3) provides that subsections (1) and (2) are civil penalty provisions. Section 317ZA contains civil penalty provisions but does not create any new offences.

Chapter 2 of the *Criminal Code Act 1995*, which sets out the default fault elements for criminal offences, does not apply to contraventions of civil penalty provisions. The civil penalty provisions in subsections 317ZA(1) and 317ZA(2) do not adopt the enforcement process framework in the *Regulatory Powers (Standard Provisions) Act 2014* and, as a result, the relevant state of mind cannot be construed by reference to section 94 of that Act.

Instead, the relevant enforcement process framework for subsections 317ZA(1) and (2) is at Part 31 of the *Telecommunications Act 1997*, and 'the question of any state of mind applicable to the proscribed conduct in the context of civil proceedings falls to be determined by way of ordinary statutory construction' (Australian Securities and Investments Commission v Whitebox Trading Pty Ltd & Anor (2017) 345 ALR 424).

In relation to a contravention of subsection 317ZA(1), the Bill contains safeguards to ensure that any carriers or carriage service providers who are issued a technical assistance notice or technical capability notice are made aware of their obligation to comply with the notice. Section 317TAA requires the Attorney-General to advise a designated service provider of their obligations to comply with a technical capability notice if they have been issued with a notice. Subsections 317MAA(1)-(2) require the

Director-General of Security, or the chief officer of an interception agency, to advise a designated service provider of their obligations to comply with a technical assistance notice if they have been issued with a notice. These provisions will ensure that providers understand their obligation to comply with the notice to the extent that they are capable of doing so in section 317ZA. There is no mental element provided for a breach of this civil penalty provision.

For subsection 317ZA(2), the intention is that a person's conduct would only be captured by that provision where the person had knowledge that the conduct was in connection with a contravention of subsection (1). To establish accessorial liability it is necessary to show that a person was intentionally involved in a contravention (*Yorke v Lucas* (1985) 158 CLR 661). Whilst subsection 317ZA(2) could apply to persons who have not themselves been issued a TAN or technical capability notice —for example a third party contractor—and consequently have not been notified of the carrier or carriage service providers obligation to comply with the notice, the provision is not intended to capture the conduct of persons who unknowingly contribute to a contravention of subsection 317ZA(1).

In addition, a person's knowledge or lack thereof may be relevant to the Court's determination of the appropriate pecuniary penalty under Part 31 of the *Telecommunications Act 1997*. Subsection 570(2) provides that, in determining the pecuniary penalty for contravention of a civil penalty provision, the Court must have regard to all relevant matters, including the nature and extent of the contravention and the circumstances in which the contravention took place. It is likely that a lesser degree of knowledge would result in a lower pecuniary penalty.

When the Australian Law Reform Commission reported on the use of criminal and civil penalties in the *Telecommunications Act 1997*, it observed that often civil penalty provisions, in contrast to criminal or 'offence' provisions, do not require proof of any fault elements (ALRC Report 108). This reflects the fact that criminal, rather than civil, liability is the appropriate sanction for conduct which involves serious moral culpability. Section 317ZA therefore reflects the standard approach to drafting civil penalty provisions.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/059*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q50) - Civil or criminal liability overseas.

Asked:

50. Some submitters advised that they will be exposed to civil or criminal liability overseas by complying with a compulsory notice with no access to the immunity extended to actions in Australia.31 For example, Apple has raised concerns that despite the defence available in 317ZB(5), a TAN or TCN may require a DCP to provide access to data, for example, that may otherwise be subject to the EU GDPR, thereby exposing the DCP to civil liability (pg 7 of submission).
a. Could the Department respond to these concerns?

Answer:

a. The defence available under proposed section 317ZB(5) is sufficiently broad enough to apply to the scenario provided. Proposed section 317ZB(5) states that a requirement under a technical assistance notice or technical capability notice which would require the designated communications provider to do an act or thing in that a foreign country that would contravene the law of the foreign country would have this defence available to them. The shaping of this provision recognises that a designated communications provider may cross many jurisdictions and conflict may occur in one of those jurisdictions and engage the defence under proposed section 317ZB(5).

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 20 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/060*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q51) - Proposed powers in Schedule 1 -

Asked:

51. Did any foreign government or foreign government agency request that the proposed powers in Schedule 1 be available for the purpose of assisting the enforcement of the criminal laws in a foreign country?

Answer:

No.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/062*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q53) - Conflicts of law.

Asked:

53. The Bill does not currently provide a mechanism to raise conflicts of laws that may be identified by a DCP. How will conflicts of laws be resolved?

Answer:

a. As previously stated, the Bill provides a platform to facilitate cooperation between issuing agencies and designated communications providers. It is expected that consultation with the designated communications provider will occur prior to the issue of a notice, especially given the requirement to consider the interests of the provider and assess whether the requirements in the notice are technically feasible. This consultation period would provide an opportunity to raise any potential conflict of laws issues.

The Bill provides a defence in civil penalty proceedings for failure to comply with a requirement under a technical assistance notice or a technical capability notice where compliance with the requirement in a foreign country would contravene the law of that country (s317ZB(5)). This means that in cases of genuine conflict of law, a notice would not (and should not) be enforceable.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/064*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q55) - Guidance to industry if Bill passed.

Asked:

55. What guidance will be provided to industry if the Bill is passed? Has the Department commenced this work? What is the timeframe for the finalisation of any industry guidance material?
a. Will the Department seek input from industry on draft guidelines before finalisation?

Answer:

a. The Department considers that guidance would be a useful adjunct to Schedule 1 of the Bill. The Department has had preliminary conversations with agencies and industry about what information would be useful to consider in the guidance, such as decision making aides, key contacts, process flow charts and template documents. There is no set timeframe for the any guidance material to be finalised. The Department considers that industry consultation would be critical to developing effective guidance.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(TOLA/070) - PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q61) - Proposed amendments to the Surveillance Devices Act (Schedule 2) warrants

61. Across the amendments proposed in the Bill, only the Crimes Act search warrants provided for in Schedule 3 explicitly authorise law enforcement to access 'account-based data' (such as data held in online email and messaging applications)? Could computer access warrants issued under the proposed amendments to the Surveillance Devices Act (Schedule 2) also be used to access this type of data? If so, why is this not explicitly set out in a similar way to Schedule 3? If not, why not?

Answer:

a. Computer access warrants under Schedule 2 cannot authorise the use of a computer or device to access account-based data that is not held in the target computer or device. Proposed section 27E sets out what a computer access warrant authorises. For example, it does not authorise the use of the computer or device to access data held in online emails or messaging applications that would not ordinarily be held on the target computer or device. However, it would authorise accessing 'chats' received through messaging applications on that computer or device.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/071*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q62) - Execution of a search warrant on premises -

Asked:

62. Unlike the 'covert' powers provided for in Schedule 2, the Explanatory Memorandum describes the search warrant powers that are proposed to be amended in schedules 3 to the Bill 'overt'. However, section 3H of the Crimes Act only requires a person to be given a copy of a warrant if they are present at the premises.
a. Is it possible that a person might never be made aware of the execution of a search warrant on their premises (potentially involving remote access to their computer or account-based data), i.e. if they are not present at the time the warrant is executed?
b. Is there any existing practice or legal requirement that would ensure an occupier of a premise subject to a search warrant is made aware of their legal rights, and their ability to make a complaint to the Commonwealth Ombudsman?

Answer:

a. Is it possible that a person might never be made aware of the execution of a search warrant on their premises (potentially involving remote access to their computer or account-based data), i.e. if they are not present at the time the warrant is executed?

In relation to section 3E search warrants, the *Crimes Act 1914* provides that:

- where the occupier of the premises or another person who apparently represents the occupier is present at the premises, they must be provided with a copy of the warrant;
- where the occupier of the premises or another person who apparently represents the occupier is present at the premises, they are entitled to observe the search being conducted; and
- if a thing is seized under a warrant or moved under subsection 3K(2), a receipt must be provided for the thing.

The cumulative effect of these provisions is that section 3E search warrants are an overt power.

In addition to these legislative requirements, the Australian Federal Police's *Functional Governance Better Practice Guide on Search Warrant Execution* requires Australian Federal Police Members to leave a copy of the search warrant and statement of rights (and where relevant, a copy of the property seizure record or property movement record) at the premises if it is being left vacant.

b. Is there any existing practice or legal requirement that would ensure an occupier of a premise subject to a search warrant is made aware of their legal rights, and their ability to make a complaint to the Commonwealth Ombudsman?

The Australian Federal Police's existing practice is to attach a statement of rights to each search warrant issued under section 3E of the *Crimes Act 1914*. The statement outlines the relevant provisions of the *Crimes Act 1914*, for example the restrictions on personal searches.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/072*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q63) - Schedule 3 proposal re section 3LA(5) of the Crimes Act

Asked:

63. Schedule 3 proposes to replace the existing office at section 3LA(5) of the Crimes Act with two new offences: an underlying offence carrying a maximum penalty of 5 years imprisonment or 300 penalty units, and an aggravated offence carrying a maximum penalty of 10 years imprisonment or 600 penalty units. The aggravated offence applies only if the offence to which the warrant relates is
a. a serious offence (defined in section 3C as an offence punishable by 2 years imprisonment or more that is not a serious terrorism offence), or
b. a serious terrorism offence (defined separately in section 3C to include most terrorism offences in the Criminal Code).

Answer:

This Question on Notice appears to be missing text. The Department is not able to ascertain the intent of the question so is unable to submit a response.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(TOLA/073) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q64) - Schedule 4 amendment to the existing offence at section 201A9(3)

64. Schedule 4 proposes an almost identical amendment to the existing offence at section 201A9(3) of the Customs Act, except the aggravated offence in this case only applies if the offence to which the relevant warrant relates is a 'serious offence', as defined in the Crimes Act. As noted above, 'serious terrorism offences' are excluded from the definition of 'serious offence', meaning that the aggravated offence in 201A(4) would not apply in most terrorism cases. Why are serious terrorism cases excluded from the proposed aggravated offence for non-compliance with a Customs Act assistance order?

Answer:

a. The exclusion of 'serious terrorism offences' from the Customs Act reflects the role and function of the Australian Border Force, including, facilitating the lawful passage of people and goods, investigations, compliance and enforcement in relation to illicit goods and immigration malpractice; and onshore detention, removals and support to regional processing arrangements. In most instances, the investigation of serious terrorism offences will be conducted by Commonwealth, State and Territory police forces.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/075*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q66) - Intention reflected in proposed section 21A of Schedule 5

Asked:

66. In paragraphs 78 and 79 of the Department's supplementary submission, it is explained that voluntary assistance requests under proposed section 21A of Schedule 5 and 'technical assistance requests' under proposed section 317G of Schedule 1 are not intended to be used interchangeably. The latter regime is intended to be used for technical requests to 'designated communications providers', whereas the former is intended to be used for non-technical requests to a broader range of persons.
a. How is this intention reflected in proposed section 21A of Schedule 5? If it is not reflected in the legislation, is there any reason why it should not be?

Answer:

a. Voluntary assistance requests under proposed section 21A of Schedule 5 and technical assistance requests under proposed section 317G of Schedule 1 are not intended to be used interchangeably. This intention is reflected in the significant difference in the scope of each regimes' application.

Technical assistance requests apply to a small subset of 'designated communication providers' and apply to technical assistance. Expanding the use of technical assistance requests to obtain non-technical information or assistance would be out of step with the rest of the framework which is limited by the things listed in section 317E, or things that are similar to those things.

Whereas section 21A of Schedule 5 can apply broadly to conduct requested by the Director-General that meets the broad objectives and restrictions of the ASIO Act itself, and the thresholds identified under subsection 21A(1).

The lack of direct comparison is a critical distinction between both voluntary assistance requests and voluntary assistance orders. However, despite the differences, there may be some cross over in the use (where both request voluntary technical assistance to access a mobile device).

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/077*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q68) - subsection 21A(1) provides "clear" thresholds.

Asked:

68. In paragraph 86 of the Department's supplementary submission, it is stated that 'subsection 21A(1) provides "clear" thresholds which must be met before an assistance order can be issued'.
a. What are these thresholds?

Answer:

a. Subsection 21A(1) relates to assistance provided in accordance with a request by the Director-General of ASIO and sets out the thresholds for applying civil liability immunity to persons or bodies engaging in that requested conduct. The thresholds are clearly set out in the Bill as the following:

- Has the Director-General requested the person or body to engage in certain conduct;
- Is the Director-General satisfied that, on reasonable grounds, the conduct is likely to assist ASIO in the performance of its functions;
- Does the conduct involve a person or body committing an offence against a law of the Commonwealth, a State or a Territory; and
- The conduct would not result in significant loss of, or serious damage, to property.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/079*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q70) - Compulsory assistance order.

Asked:

70. Proposed section 34AAA(2)(c)(i) provides that a compulsory assistance order may be issued to a person if he or she is 'reasonably suspected of being involved in activities that are prejudicial to security.'
a. Does there need to be a nexus between the prejudicial activities that this person is involved in and the security activities that are subject of the particular warrant?

Answer:

a. Yes. Section 34AAA(2)(c)(i) allows for requests to specifically target persons of interest who are suspected of being involved in activities that are prejudicial to security. This is necessary to ensure that the person of interest can be subject to these orders and there would, in most circumstances, be the expectation that there would be a nexus between the specified person under section 34AAA(2)(c)(i) and the underlying actions under paragraph 34AAA(1)(a).

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/081*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q72) - Paragraph 102 of the Department's supplementary submission

Asked:

72. In paragraph 102 of the Department's supplementary submission, it is noted that 'where the computer or data storage device is on premises, it is implicit that the person will provide assistance at the time of the warrant's execution and in a manner consistent with the issued warrant'.
a. In such a situation, absent the requirements under section 34AAA(3), how will a person know for how long, and under what conditions, an order will need to be complied with?

Answer:

a. Where a compulsory assistance order is made for a computer or data storage device on premises, it would ordinarily be that persons identified as a person with knowledge of that computer or computer system who could assist, they would generally be expected to do so. However, as provided in the supplementary submission, the additional oversight measures are necessary in these rare instances as the warrant relates to a different location which has not been *envisaged by the issued warrant*.

In the scenario offered by the Committee, the order would need to be complied with in a manner consistent with the underlying order. For example, where the compulsory assistance order is done so for the purposes of a warrant under section 25A, should the person not be able to comply at the time of the execution of that warrant and the device is seized, the person would only have to comply until the device is seized and removed. ASIO may need to seek a further compulsory assistance order to compel someone to assist in compliance with the safeguards under proposed section 34AAA(3).

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/082*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q73) - Method and mode in which compulsory assistance orders must be issued.

Asked:

73. Is there any reason why proposed section 34AAA should not contain provisions regarding the method and mode in which compulsory assistance orders must be issued?

Answer:

a. Not including the particular method and mode in which a compulsory assistance order must be issued accords with the similar Commonwealth statutory compulsory assistance orders, such as those under existing section 3LA of the *Crimes Act 1914*. This maintains a degree of flexibility in how best to serve the order while recognising that the person will need to be made aware of the order before compliance could be achieved.

Any prosecution for non-compliance with the order would take into account and consider whether there were any deficiencies in the method and mode in which a compulsory assistance order was issued. The Commonwealth Director of Public Prosecution will also apply the *Prosecution Policy of the Commonwealth*.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/083*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q74) - proposed sections 21A and 34AAA.

Asked:

74. Is there any reason why do not contain provisions regarding the variation or revocation of a voluntary assistance order or a compulsory assistance order?

Answer:

a. The Department notes that the voluntary assistance provided for under proposed section 21A is just that, voluntary. It is unnecessary to require a voluntary request to have a specific process concerning the variation or revocation of that request where that assistance is help given to Australian Security Intelligence Organisation.

It is also unnecessary to step out variation and revocation provisions for compulsory assistance orders under the proposed section 34AAA given the implied power to amend or repeal orders made under section 43 of the Acts *Interpretation Act 1987*.