Australian Government
Department of Home Affairs

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

Department of Home Affairs responses to Questions on Notice.

Index

Index

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/016*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q7) - Unlocking Encrypted Communications.

Asked:

7. A large number of submitters have cautioned that unlocking encrypted communications even on one device or platform used by a single individual would significantly compromise the security for a larger number of users or, in some circumstances, all users.5 Does the Department reject this evidence? If so why?
a. Can you provide the assurance to the Committee that security of many will not be compromised by accessing the encrypted communications of a few?

Answer:

Requiring a provider to unlock encrypted communications on a device, where they are currently not able to do so, is not within scope of the Bill. Requirements to build such a capability interact with two prohibitions; (1) the express limitation against 'decryption capabilities' into forms of electronic protection in proposed section 317ZG(2), and (2); the exclusion of listed act or thing in proposed section 317E(1)(a) ('removing a form of electronic protection applied by, or on behalf of, a provider') from the things that any technical capability notice can require (see 317T(4)(c)(i)).

The Department understands the question to refer to a situation where forms of electronic protection (like encryption or passwords) have effectively secured communications on a device or a service. As drafted, the Bill could not require a provider to construct a targeted decryption or unlocking capability that would remove electronic protection applied by them. As such the evidence provided to the Committee on this issue is not relevant to the operations of the Bill.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/017*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q8) - data retention measures.

Asked:

Stakeholders have expressed some concern about the ability for industry assistance measures to expand the scope of data retention measures. The Bill establishes a limitation on the ability for a technical capability notice that would otherwise require a provider to retain information that is specified in s 187AA of the TIA Act (proposed section 317T(10). Elsewhere the TIA Act establishes a clear prohibition against the retention of web-browsing history (section 187A(4)(b)) and over-the-top services (section 187A(4)(c)). a. Is it intended that the industry assistance measures would extend the scope of data that might be (compulsorily or voluntarily) retained by providers?
b. If it is the intention, what is the policy reason for this inclusion?

Answer:

a. It is not the intention that the industry assistance measures extend the scope of data that might be kept. The limitation in section 317T(10) is designed to ensure that the data retention obligations as currently expressed in the Telecommunications (Interception and Access) Act 1979 (TIA Act) cannot be replicated through a technical capability notice. Other capabilities relating to data will be subject to the extensive decision-making requirements of a notice.

The Department notes that subsections 187AA(2) enables the Minister to make a declaration modifying the types of data retained in the table in 187AA. Any additional data sets would be added through this established mechanism or legislative amendment as envisaged by 187AA(4).

b. It is not the intention.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA\018*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q9) TCN Notices

Asked:

9. Schedule 1 to the Bill contains a limitation (317T(10)) that would prevent a technical capability notice (TCN) from being issued to a designated communications provider that required telecommunications metadata to be retained, where that provider is regulated under the TIA Act and the information is a kind that is regulated under the data retention regime. Schedule 1 also includes a limitation (317ZH) that would prevent a technical assistance notice (TAN) or a TCN from requiring a designated communications provider to disclose metadata that would ordinarily require an authorisation under the TIA Act.
a. For designated communications providers that are subject to the TIA Act, could a TCN be issued that would require types of metadata that are excluded from the data retention regime to be retained—for example, browsing histories?
b. Could a TCN be issued to a designated communications provider that is not subject to the TIA Act—such as an 'over-the-top' service provider like Gmail and Facebook Messenger—which required that provider to retain telecommunications metadata?
c. Could a TAN or TCN be issued to a designated communications provider that is not subject to the TIA Act—such as an 'over-the-top' service provider like Gmail and Facebook Messenger—which required that provider to disclose telecommunications metadata to government agencies outside the TIA Act process?
d. Can the Department please provide a written briefing on the avenues available for agencies to collect metadata under any Commonwealth law?Can the Department confirm that the states and territories do not have the constitutional power to legislate in their own right on this matter?

Answer:

a. The limitation in section 317T(10) operates prevent a technical capability notice to replicate existing data retention obligations on a designated communications provider. Part 5-1A of the Telecommunications (Interception and Access) Act establishes a process by which the Minister can add additional data sets, like browsing history, to the data retention regime. This is the applicable process to follow for extending the scope of the data retention regime.

b. The limitation in section 317T(10) applies to notices served on all designated communication providers - not just carriers or carriage service providers to which Part 5-1A of the Telecommunications (Interception and Access) Act applies.

Communications and their metadata are largely carried through the services identified in Part 5-1A. Accordingly, the prohibition in 317T(10) would restrict the ability of a technical capability notice to impose data retention requirements of a kind expressed in Part 5-1A on the broader category of designated communications provider.

c. No. The limitation in section 317ZH clearly prohibits this. It reads that a technical assistance notice or technical capability notice has no effect if it required a designated communication provider to do an act or thing for which a warrant or authorisation was required under a law of the Commonwealth, State or Territory. Subsection 317ZH(2) ensures that, for the purposes of this prohibition, these laws can be taken to apply both within and outside Australia. Paragraph 317ZH(2)(b) extends the status of carriage service provider to all designated communications providers under Schedule 1 of the Bill.

The combined effect of these limitations is to extend the prohibition on disclosing metadata that carriage service providers have under the Part 13 of the *Telecommunications Act 1997* to all providers. This means that, to disclose metadata, a valid authorisation which forms an exception to this prohibition is required. Chapter 4 of the Telecommunications (Interception and Access) Act is one such exception but its territorial limitations still apply and, as such, they may not be issued to providers who are not already required to respond to them. Section 280 of the *Telecommunications Act 1997* is another – however, as 'enforcement agencies' under that Act, the entities empowered by Schedule 1 will not be able to use section 280 to authorise disclosure unless a warrant is also present. The applicable warrants will also have territorial limitations.

In summary, the effect of section 317ZH is to extend prohibitions on disclosing metadata to all designated communications providers. A warrant or authorisation will be required to authorise disclosure and a technical assistance notice or technical capability notice cannot act in replacement of this requirement. A technical assistance notice or technical capability notice could not be used to require disclosure of metadata inside or outside the Telecommunications (Interception and Access) Act process.

d. The Department will provide a written briefing to support the upcoming review into data retention in April 2019.

The Department will need to seek legal advice with regards to the constitutional validity of states or territory legislation in this area.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/023*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q14) Systemic weakness/systemic vulnerability

Asked:

14. Why is the limitation on systemic weakness/systemic vulnerability only available to assistance with electronic protection and is not extended to other types of assistance that may fall within a 'listed act or thing' as defined in section 317E or 'listed help' as defined in section 317T(4)?

Answer:

As noted in the Department's response to questions received on 23 October 2018, the Department considered that leaving the limitation at building or implementing a systemic weakness or vulnerability would be unnecessarily ambiguous (what is being weakened?) and the term electronic protection establishes a helpful anchor. Electronic protections are designed to reduce the risk of unauthorised interference with a person's services or devices, therefore weaknesses or vulnerabilities that erode these protections are the relevant ones.

The policy intent of the limitation on systemic weaknesses / systemic vulnerabilities is to ensure that the security of devices and services remain intact. This is best achieved by prohibiting the compromise of the very measures, the electronic protections, put in place to protect the devices and services of users.

The term electronic protection is purposefully broad. An ordinary understanding would allow it to capture passwords, encryption methodology and other security layers and forms of authentication. The Department has not defined it to allow scope for providers to submit and argue that particular features of devices and services do indeed protect the device from unauthorised interference.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/030*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q21) - Capability under the TCN

Asked:

21. Once a capability is built under a TCN, what will govern the use of that capability by a requesting agency?
a. What matters would be considered and by whom and to what standard before that capability is deployed?
b. The relevant objective test is only applied at the time the decision-maker is considering issuing the notice. What matters would be considered, by whom, and to what standard for later or subsequent deployments beyond the original matter that was considered prior to the notice being issued?

Answer:

Requirements for the actual use of that capability must be set consistent with the decision-making within the technical capability notice, taking into account reasonableness, proportionality, practicality and technical feasibility. The decision-making criteria sections (see 317ZAA) the interests of law enforcement, security, the provider and privacy/cybersecurity are taken into account.

Section 317ZK enables agencies, the Government and providers to agree to the terms and conditions of compliance with requirements in a notice. In circumstances where agreement cannot be reached, this section establishes an arbitration process. This process allows multiple agencies to determine how best to utilise the capability and cooperate with the provider. Through these provisions the Bill allows for clear, flexible terms to be set and documented that allow for mutual understanding amongst all parties.

A technical capability notice allows for both the construction of the capability and its subsequent use. This removes the need to issue a technical capability notice to support the use of a higher threshold technical capability notice. If the use goes to the collection evidence of intelligence, the actual collection will need to be supported by an underlying authority - like a warrant.

a. Matters going to a capability will be considered by all relevant parties. The Government & Agencies (represented by the applicable costs negotiator) will agree to the terms and conditions with the relevant designated communications provider. In a technical capability notice the applicable costs negotiator is the person specified in the notice (see 317ZK(16)). This is deliberately flexible to allow a person who can best represent the Government at multiple levels to be nominated. The need to agree upon the terms and conditions, or failing that the mechanisms for determination by the third-party arbitrator, will function to ensure negotiations are not one-sided and reach standards amenable to all parties.

If deployment is for an activity that requires a warrant or authorisation, the legal standards identified in the relevant statue will need to be met.

b. Terms and conditions of compliance, including compliance with requests for subsequent deployment of a capability, are established in accordance with section 317ZK and relate to the initial requirements of a notice which must meet the decision-making thresholds.

It is anticipated that many capabilities will be designed to facilitate the execution of an underlying warrant or authorisation. In these cases, it will be the underlying warrant requirements that will principally govern its use. In the case of a surveillance device for example, an eligible Judge or nominated Administrative Appeals Tribunal member must be satisfied of particular standards in a surveillance device warrant before its execution. In this scenario the capability is facilitating the execution of a surveillance device that has met statutory thresholds.

There is a standing requirement that the Attorney-General must revoke the technical capability notice if the Attorney-General is satisfied that the requirements imposed, including requirements for continued use, are not reasonable, proportionate, practical and technically feasible. This will ensure that capabilities continue to be governed by considerations akin to the original decision-making criteria or be subject to revocation.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/036*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q27) - ASIO and requests outside of the functions or powers of ASIO?

Asked:

27. For the relevant decision maker to issue a notice/request, the notice/request must be directed towards the 'performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth … so far as the function or power relates to a relevant objective'. For the purposes of a request/notice sought or issued by ASIO, could the Department confirm whether ASIO could seek/issue that request outside of the functions or powers of ASIO?
a. Would ASIO, for example, be limited in seeking a notice/request for the exercise of a function outside of the ASIO Act?
b. Would ASIO be able to seek/issue a technical assistance notice or technical capability notice for the purpose of assisting another agency under section 19A of the ASIO Act, even if that other agency would not be authorised to seek/issue such a request or notice itself?

Answer:

a. Australian Security Intelligence Organisation would only seek the request/notice under sections 317G(2) and 317L(2) in relation to the performance of an Australian Security Intelligence Organisation function. In accordance with Section 20(a) of the *Australian Security Intelligence Organisation Act 1979*, the Director-General is required to take all reasonable steps to ensure that the work of the Organisation is limited to what is necessary for the purposes of the discharge of Australian Security Intelligence Organisation's functions.

b. Under section 19A the *Australian Security Intelligence Organisation Act 1979*, Australian Security Intelligence Organisation may co-operate with and assist Australian Secret Intelligence Service, Australian Signals Directorate, Australian Geospatial-Intelligence Organisation, a law enforcement agency, and prescribed Commonwealth and State authorities, in the performance of their functions. Under section 19A arrangements, Australian Security Intelligence Organisation may provide such resources as staff, or linguistic or technical services to those agencies or authorities.

Australian Security Intelligence Organisation's current approach to section 19A is that it does not use an Australian Security Intelligence Organisation specific power for the sole purpose of assisting another agency with the performance of their functions. We note, however, it may be arguable that section 19A allows Australian Security Intelligence Organisation to seek/issue a technical assistance notice or a technical capability notice for the purpose of assisting another agency.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/038*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q29) - Criminal laws in force in a foreign country.

Asked:

29. The relevant objective test for each type of notice (TAR, TAN and TCN) specifies that a relevant objective will be 'assisting the enforcement of the criminal laws in force in a foreign country'. Outside the limited forms of assistance that can be provided in certain circumstances under the Mutual Assistance in Criminal Matters Act 198718, does any existing Australian law enable an Australian agency to exercise compulsive powers against a third-party (who is not the target or subject of an investigation) for the purpose of the enforcement of the criminal laws in force in a foreign country?

Answer:

Yes. Section 313 of Telecommunications Act requires a carrier or carriage service provider to give help reasonably necessary to an authority of the Commonwealth, State or Territory for particular purposes. One of these purposes is enforcing the criminal laws in force in a foreign country. A failure to comply with obligations under this section is an enforceable breach of a carriers licence and attracts significant penalties upwards of AUD$10 million. Similarly, under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*, Australian Federal Police officers can request the disclosure of telecommunications data from carriers or carriage service providers for the purpose of enforcement of the criminal law of a foreign country. Compliance with a valid authorisation is compulsory.

A number of other legislative regimes are relevant here. Under the Mutual Assistance in Criminal Matters Act 1987 Australia can provide assistance to foreign countries for criminal investigations, prosecutions and proceeds of crime proceedings.

Australia can also provide assistance in the form of coercive or compulsive powers to the International Criminal Court and any established international war crimes tribunals. The *International Criminal Court Act 2002* (ICC Act) and the *International War Tribunals Act 1995* (IWCT Act) provides the framework for the exercise of coercive and compulsive powers for these international bodies.

Under the *Australian Federal Police Act 1979* Australia can also provide police to police assistance but this assistance does not extend to coercive or compulsive powers.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/041*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q32) - The UK Investigatory Powers Act

Asked:

32. The UK Investigatory Powers Act provides for a form of merits review by way of an DCP-equivalent seeking a review by the Secretary of State after the notice is issued (the Secretary must then consult the Technical Advisory Board and a Judicial Commissioner).19 Why was this approach not taken in the development of the Bill?

Answer:

The technical capability notices in this Bill contain robust consultation and decision-making requirements, including a lengthy consultation period, which is anticipated to reduce the need for merits review (see 317(W)). Representations made by the provider and an appointed technical expert must be considered before the issuance of the notice. This process will allow for a provider's expressed concerns and technical determinations to be factored into the initial technical capability notices.

The United Kingdom technical capability notices also serve a different function to the Bill's Technical Capability Notices. The Department understands that the United Kingdom uses technical capability notices to establish the same core interception and surveillance capabilities that Australia governs through other legislative requirements, like the *Telecommunications (Interception and Access) Act 1979*. Given how significant these core capabilities (forming the very backbone of lawful interception) it may be appropriate in a United Kingdom context to allow for the review process set out in the *Investigatory Powers Act 2016 (United Kingdom)* (United Kingdom Institute of Public Accountants).

Further, the ongoing requirement that the Attorney-General must revoke a notice if no longer satisfied of its reasonableness, proportionality, practicality and technical feasibilities enables providers to make further representations to the Government at a later date with regards to the ongoing suitability of technical capability notices requirements.

In general terms, exclusion of merits review processes for decisions of this nature is a consistent feature of the Australian legislative landscape. For example, decisions made under the *Intelligence Services Act 2001* and the Australian Security Intelligence Organisation Act are excluded from merits review. Decisions of a law enforcement and national security nature were identified by the Administrative Review Council in its publication *What decisions should be subject to merits review* as being unsuitable.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/047*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q38) - AHRC detailed submission on immunity provisions

Asked:

38. The AHRC has provided a detailed submission on immunity provisions in Schedule 1.23 Could the Department please respond to each concern raised on this issue?
a. In addition, could you clarify whether a DCP will have immunity despite a non-enforceable notice (for example a notice that had no effect by virtue of the limitation provisions) and the subsequent and purported compliance by that DCP with that non-enforceable notice?
b. In such circumstances, could you also advise whether an individual who had been negatively impacted by a data breach for example would be able to seek civil remedy for such damage?

Answer:

The Australian Human Rights Commission raise important points concerning the need to justify the use of certain immunities. The Bill specifically shapes the civil immunities, for example, around the necessity that any actions taken in compliance, or purported compliance, providers should not subject them to the possibility of legal action due to civil liability.

This is not unusual as other Commonwealth statutes apply civil immunity for actions done in good faith. For example, section 313 of the *Telecommunications Act 1997* includes similar immunities from action or other proceedings and states that *'[a] carrier or carriage service provider is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith…'*.

The Australian Human Rights Commission also specifically question the appropriateness of providing criminal immunities for technical assistance requests. These criminal immunities ensure persons are not criminally responsible for an offence against subsection 474.6(5) of the *Criminal Code Act 1995* (Criminal Code) if the conduct of the person is in accordance with a technical assistance request, or in compliance with a technical assistance notice or a technical capability notice. Application to the voluntary assistance requests recognises that a person acting in good faith in the course of his or her duties should not be criminally liable where the conduct is reasonable in the circumstances for the purpose of performing the duty. Further, if criminal liability were excluded from the technical assistance request regime it would make the voluntary framework inherently riskier for people wanting to assist law enforcement and security agencies. This could have the effect of making voluntary cooperation less appealing.

a. Yes. Where actions were undertaken by a development control plan in purported compliance with a notice, section 317ZJ ensures that where acts are done so in good faith, there should be applicable immunities.

b. No. Where actions were undertaken by a development control plan in purported compliance with a notice and in good faith, section 317ZJ would provide immunity. However, the Bill does not prevent the application of other statutory schemes, such as the mandatory data breach notification scheme, from applying. Proposed paragraph 317ZF(3)(c) allows for disclosure of information in accordance with any requirement imposed by a law of the Commonwealth.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/048*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q39) - Technical definitions

Asked:

39. The terms 'technical assistance notice information', 'technical assistance request information' and 'technical capability notice information' all include the following in their definitions: "any act or thing done in accordance with a technical assistance request/technical assistance notice/technical capability notice".24
a. Do these terms cover the actual capability, for example, that would be developed under a TAR or TCN? That is, would a DCP be prohibited from disclosing information that outlined the new capability that was developed by virtue of the notice?

Answer:

a. Yes. A capability would be developed in accordance of a technical capability notice. Accordingly it is expected that disclosing the capability itself would be, in effect, revealing information about the requirements imposed by a technical capability notice and any acts or things done in compliance with a technical capability notice.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/055*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q46) - Sharing of information between agencies

Asked:

46. Could a capability that is developed under a TCN requested by ASIO (and authorised by the Attorney-General) be shared with Australian Signals Directorate28 or Australian Secret Intelligence Service?29
a. If that information or capability could be shared, what existing Commonwealth law would govern the decision to share that information?
b. If it was considered inappropriate that these agencies be included in the list of agencies that can issue a TAN or request that the Attorney-General issue a TCN, why should that information or capability obtained under those notices be shared with those agencies?

Answer:

a. Yes. Australian Security Intelligence Organisation can communicate intelligence (a subset of information) relevant to security for purposes relevant to security. Sections 18(4A) and 19A(4) of the *Australian Security Intelligence Organisation Act 1979* provide for lawful communication of information in circumstances where there is a nexus to the functions of the recipient agency. Section 18(3) would also enable communication of information if the Director-General, or a person authorised by the Director-General, is satisfied that the national interest requires the communication. We also note under section 317ZK a communications provider could seek to negotiate a term of compliance with a technical capability notice which restricts Australian Security Intelligence Organisation sharing the capability with third parties or other agencies.

b. The fact that Australian Signals Directorate and Australian Secret Intelligence Service cannot issue a technical assistance notice or that the specified acts or things in a technical capability notice cannot go to directly helping Australian Signals Directorate and Australian Security Intelligence Organisation reflects an important distinction. The primary purpose of these coercive powers are connected to the key law enforcement and security agencies explicitly included in the regime. Given the intelligence functions and offshore focus of Australian Signals Directorate and Australian Secret Intelligence Service, the Department did not consider it suitable that they have the capacity to exercise these coercive powers. By contrast, Australian Security Intelligence Organisation and law enforcement agencies have robust domestic powers and legal frameworks in place that moderate the coercive activities.

However, where information that has already been obtained, or a capability developed, for the purposes of these domestic-focused agencies appears relevant to the functions of Australian Signals Directorate and Australian Secret Intelligence Service, there is an expectation that resources are deployed in the national interest. The Bill allows Australia's intelligence agencies to work closely together to protect Australia and remove arbitrary barriers to intelligence sharing. The use of any information or capability must be consistent with the robust statutory frameworks of the intelligence agencies and subject to oversight by the Inspector General of Intelligence and Security.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/061*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q52) - Proposed industry assistance powers

Asked:

52. As a matter of practice, how would a relevant agency authorised under Schedule 1, exercise its proposed industry assistance powers for the relevant objective of enforcing the criminal laws of a foreign country? What representations would need to be made for that objective to be satisfied? How would this relevant objective interact with the existing mutual legal assistance regime?

Answer:

Established channels between Australia and other countries would continue to guide representations between Australian authorities and overseas authorities. For example, central authorities for mutual assistance receive and action requests for assistance relating to criminal investigations. Agencies may also learn of the need for this assistance on a police-to-police basis.

The relevant objectives test require a technical assistance request, technical assistance notice or technical capability notice to specify acts or things relating to the performance of a function or power under law and relevant to enforcing the criminal laws in force in a foreign country. Therefore assisting the foreign authority must be consistent with existing statutory functions of the agency. Australian authorities will consider whether the requested assistance falls within their establish duties and, consistent with standard practice, request sufficient information from the overseas authority to determine the nature of the foreign criminal offence and the circumstances surrounding it. Limitations in an Agencies' enabling legislation, in addition to whole-of-government policies further guide how authorities act upon foreign requests for assistance.

The inclusion of the objective of '*assisting the enforcement of a criminal law in force in a foreign country*' complements Australia's mutual legal assistance regime.

The *Mutual Assistance in Crime Matters Act 1987* governs Australia's mutual legal assistance regime. Under the *Mutual Assistance in Crime Matters Act 1987*, Australia can only provide assistance to foreign countries for criminal investigations, prosecutions and proceeds of crime matters.

Section 6 of *Mutual Assistance in Crime Matters Act 1987* provides that “This Act does not prevent the provision or obtaining of international assistance in criminal matters other than assistance of a kind that may be provided or obtained under this Act.”

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/063*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 1 (Q54) - Clarifying Lawful Overseas Use of Data Act (the CLOUD Act)

Asked:

54. Professor Pfefferkorn has provided a supplementary submission to the Committee on the Bill's interaction with the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), advising:
a. that the extraterritorial provisions of the Bill alone are not sufficient to legally obtain data held in the United States. Such information can only be legally obtained from US providers by going through MLAT (letters rogatory) or the CLOUD Act Agreement process;32
b. that aspects of the Bill may present challenges for Australia's negotiations to enter an executive agreement with the United States for access to data held within the United States under the CLOUD Act;33
c. that a request for a US provider for voluntary actions would be unenforceable;34
d. that the CLOUD Act does not create any stand-alone legal authority for a foreign government to mandate any action by a US provider, but rather removes prohibitions against disclosure that otherwise exist by way of the Electronic Communications Privacy Act;35
e. that even if an executive agreement was signed between Australia and the United States, any request to a US provider would have to comply with the CLOUD Act and that nothing in the CLOUD Act authorises the foreign government to mandate disclosure by the US provider;36 and
f. that any executive agreement between Australia and the United States would be 'flatly barred' from creating any obligation that providers be capable of decrypting data'.37 Could the Department respond to each of these points raised by Professor Pfefferkorn?

Answer:

The Department noted Ms Pfefferkorn's of Standford's Centre for Internet and Society testimony to the Committee.

The Department recognises the value of ongoing mutual legal assistance processes through existing bilateral arrangements between the United States and Australia. As Ms Pfefferkorn clearly states in her submission, this specific channel of formal international crime cooperation will remain, whether or not the Australian Government successfully negotiates an executive agreement under the guidance of the Clarifying Lawful Overseas Use of Data Act. Ms Pfefferkorn acutely acknowledges the well-known complexities and frustrations experienced with the increasing pressure on formal international crime cooperation frameworks globally.

However, many of Ms Pfefferkorn's points appear to assume that the purpose of Schedule 1 is to require disclosure of user data and content from United States providers. This is not the case. The Bill cannot compel United States providers to disclose content or non-content data. Schedule 1 of the Bill is to designed to provide a framework of assistance for United States providers in relation to services or devices in Australia. It does not seek to compel those providers to do things under the law of the United States. It seeks to ensure that where United States providers aim to provide a service or device in Australia, there is a mechanism under Australian law to oblige those providers to assist in some way or form. Concerning enforceability, the Bill provides an enforcement mechanism by allowing non-compliance to be taken before the Federal Court of Australia. This includes foreign service providers captured by the definition of 'designated communications providers'. Any outcome from legal action taken in the Federal Court of Australia would only apply in the Australian jurisdiction.

The Bill does not aim to impact specific United States law within their jurisdiction. This is clearly articulated by the defence under proposed section 317ZB which creates an exception to non-compliance where a designated communications provider (other than a carrier or carriage service provider) would contravene local laws of their jurisdiction. The Department understands that the Clarifying Lawful Overseas Use of Data Act and respective requirements only permit mutual recognition of orders which cover the disclosure of content or non-content data, not necessarily any obligations that would otherwise apply to domestic service providers and not be permitted under United States law, including the Clarifying Lawful Overseas Use of Data Act.

On the point of encryption, the Bill cannot create any obligation that providers be capable of decrypting data, including United States providers. Section 317ZG clearly prohibits this as does the Bill's restriction on technical capability notices from removing a form of electronic protection (see subparagraph 317T(4)(c)(i)). The Department takes this as an opportunity to acknowledge the great benefits an executive agreement would have on timely access to electronic data held by both Australian and United States service providers respectively. This timely access is an essential component to effects to protect the community and combat serious crime. Should there be interest from the United States to pursue an executive agreement with Australia, the Department would work proactively to address any issues raised as to the interaction between Australia's laws and the requirements under the Clarifying Lawful Overseas Use of Data Act.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/068*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 2 (Q59) - Search warrants issued

Asked:

59. How many search warrants were issued under section 3E of the Crimes Act and section 198 of the Customs Act in 2017–18? What agencies used these powers, and how many times? What offences did these search warrants relate to.

Answer:

Similar to the above response, the Australian Federal Police notes that obtaining these statistics would require a manual search of all operational records. This would be extremely labour intensive and require an unreasonable diversion of resources to search every holding.

Search warrants issued under Section 3E of the *Crimes Act 1914* must be executed by a constable (i.e. a member or special member of the Australian Federal Police or a member of a State or Territory police agency). Australian Government Departments and Agencies may request assistance from the Australian Federal Police to execute a section 3E search warrant on their behalf. In instances where the Australian Federal Police executes a search warrant on behalf of another agency, the warrant and seizure of evidential material must still be wholly for the purpose of a criminal prosecution and/or related action under the *Proceeds of Crime Act 2002* and not a disciplinary, administrative or civil proceeding.

The ABF notes that 217 section 198 *Customs Act 1901* warrants were issued in the 2017/2018 financial year. Section 198 *Customs Act 1901* search warrants are utilised when there are reasonable grounds for suspecting that there is evidential material in relation to offences committed against the *Customs Act 1901* or other offences as defined in section 183UA. Section 198 warrants can only be issued to, and executed by an officer of Customs.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/065*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 2 - (Q56) - Computer access warrants.

Asked:

56. How many computer access warrants were issued under the existing provisions of the ASIO Act in 2017-18? How many of these warrants also required a telecommunications interception warrant to be issued?

Answer:

This information is classified and will be provided to Committee through secure channels.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/066*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 2 (Q57) - Surveillance device warrants issued to law enforcement in 2017–18?

Asked:

57. How many surveillance device warrants were issued to law enforcement in 2017–18?What proportion of these warrants involved viewing information held on computer devices? What offences were these warrants issued in relation to?

Answer:

The *Surveillance Devices Act 2004* annual report contains statistics for surveillance device warrants issued to Commonwealth, state and territory law enforcement. One type of device, 'data surveillance devices' are used to monitor the input into or out of a computer.

Figures setting out the number of surveillance device warrants issued for the 2017-2018 period have not yet been collated. During the 2015-2016 period, 1170 surveillance device warrants were issued. During the 2016-2017 period, 1113 surveillance device warrants were issued.

During the 2015-2016 period, seven surveillance device warrants were issued to view data and 1123 surveillance device warrants were issued to authorise multiple kinds of surveillance (optical, listening and data etc...). During the 2016-2017 period, two surveillance device warrants were issued to view data and 1054 surveillance device warrants were issued to authorise multiple kinds of surveillance.

The Department notes that, given the often multifaceted nature of investigations, it is far more common for agencies to apply for composite multiple surveillance devices which mix types of surveillance rather than a limited single type of device. It is understood that data tracking is frequently used under these composite multiple applications.

The annual reports do not collate the specific offences for which surveillance device warrants are issued. Surveillance device warrants can be used to assist in the investigation of Commonwealth offences which carry a maximum penalty of at least three years imprisonment and state offences with a federal aspect which carry a maximum penalty of at least three years imprisonment. Additionally, surveillance device warrants may also be issued to investigate defined additional offences in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, the *Financial Transaction Reports Act 1988*, *Fisheries Management Act 1991* and the *Torres Strait Fisheries Act 1984*, offences against laws of the Commonwealth, states and territories arising from integrity operations which carry a maximum penalty of at least 12 months imprisonment or an offence prescribed by the regulations.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/067*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 2 (Q58) - Assistance orders issued in the last 10 years

Asked:

58. How many 'assistance orders' have been issued under the existing provisions of each of the Crimes Act and the Customs Act in the last ten years? What offences were these orders issued in relation to?

Answer:

Information relating to investigations and the exercise of police powers seizures are recorded on the Australian Federal Police's Police Real-time Online Management Information System (PROMIS). However, the Police Real-time Online Management Information System system does not enable the generation of statistics on assistance orders. To obtain statistics on assistance orders issued under the *Crimes Act 1914* in the last ten years would require a manual search of all operational records. This would be extremely labour intensive and require an unreasonable diversion of resources to search every holding.

Similarly, the Australian Border Force (ABF) notes that extracting the number of assistance orders issued within the last ten years would require manual audit of all warrant activity undertaken within that time period. This request would represent an unreasonable diversion of resources that would impact operational areas of the ABF.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/069*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 2 (Q60) - Search warrants involving data on computers

Asked:

60. What proportion of search warrants issued under the current provisions of Crimes Act and the Customs Act involve law enforcement accessing data held on computers? What are the current limits on the ability of law enforcement to access data held on computers, both in terms of 'relevant data' and 'account-based data', as defined in the Bill?

Answer:

While a range of evidential material may be seized under a *Crimes Act 1914* search warrant, the vast majority, if not all, search warrants involve material in electronic form, be it computer, mobile phone, vehicle and GPS systems or removable digital storage (e.g. USB thumb drives, portable hard-drives, writeable CDs and DVD's). Smartphones (including Apple and Android) are all associated with an online account which enables the device to be activated and to receive updates. As a result, the vast majority of connected smart devices will access or store data on remotely hosted accounts. Increasingly more data is remotely hosted in "account-based" services, to enable users to access data across multiple devices and to ensure that data can be recovered in the event the device is lost or damaged.

This account based data can be a rich source of evidence and may include information that has subsequently been deleted and is therefore no longer accessible through examination or seizure of the device itself. Currently search warrant provisions require this data to be accessed using equipment located or moved from the search warrant premises. This access has the potential to taint evidence located on the device, or may not be accessible in the event the device is not located, is damaged or is otherwise unable to be unlocked.

Section 198 *Customs Act 1901* search warrant authorises the executing officer or a person assisting to, amongst other things, search for evidence at the warrant premises, including electronic devices located on the premises of which the warrant was issued. There are limitations on accessing data not held on the devices. In particular, the *Customs Act 1901* is limiting in that despite the fact that it provides for the use of electronic equipment on or in a premises and allows access to “data not held at the premises”, it does not however provide provisions for the critical element of accessing “data not held at the premises” once a device has been moved to another place. This provides additional challenges for the ABF in accessing data that may be stored in a cloud based format that is located after the devices have been moved.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/074*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 5 (Q65) - Proposed section 21A(1)(b)

Asked:

65. Proposed section 21A(1)(b) requires the Director-General to be satisfied, on reasonable grounds, that the requested conduct is likely to assist ASIO in the performance of its functions.
a. To reach the state of satisfaction required before issuing a voluntary assistance request, what are some of the factors, if any, that the Director-General must consider?
b. Does this require the Director-General to consider the impact on third-party rights as a result of granting civil immunity?

Answer:

a. When exercising his powers, the Director-General applies the ordinary obligations attaching to executive decision making. Noting the request needs to be lawful, reasonable, without bias, proportionate and within the confines of the relevant power etc. The Attorney-General's Guidelines[1] are also applicable to the Director-General's decision making.

b. Not expressly. We note, however, the oversight of the Inspector-General of Intelligence and Security in relation to such a request. Inspector-General of Intelligence and Security considerations include propriety as well as legality.

[1] https://www.asio.gov.au/sites/default/files/Attorney-General's%20Guidelines.pdf

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/076*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 5 (Q67) - Limitations to civil immunity

Asked:

67. In paragraph 82 of the Department's supplementary submission, it is noted that '[l]imitations to civil immunity are clearly expressed and do not cover significant loss of, or serious damage to, property or conduct that constitutes an offence. The Department considers that these limitations are sufficiently broad to capture instances of meaningful harm to other persons.'
a. What is the basis for assessing 'meaningful harm to other persons'?
b. Do these limitations cover pure economic loss, or conduct resulting in physical or mental harm or injury?
c. If not, why have these been excluded?

Answer:

a. The term 'meaningful harm' is not used in the Act. This was simply a term was used by the Department to describe the range of conduct that immunity does not apply to, i.e. conduct referred to in subparagraphs 21A(1)(1)(d) and (e) and 21A(5)(d) and (e) of Bill.

b. Immunity is not extended to conduct which would amount to an offence against a law of the Commonwealth, a state or a territory. Commonwealth, state or territory offences could capture conduct that involves physical or mental harm or injury. This is in addition to the limitation on immunity for conduct which results in significant loss of, or serious damage to property.

The policy intention is to cover pure economic loss and conduct resulting in physical or mental harm or injury within the immunity. This is consistent with a plain reading of the section and the current operation of similar powers such as section 35K of the Australian Security Intelligence Organisation Act.

c. See above.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/078*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 5 (Q69) - Proposed section 34AAA(2)(b).

Asked:

69. Proposed section 34AAA(2)(b)requires the Attorney General to be satisfied that there are reasonable grounds for suspecting that access by ASIO to data held in, or accessible from, the computer or data storage device will substantially assist the collection of intelligence…that is important in relation to security.
a. To reach the state of satisfaction required before issuing a compulsory assistance order, what are some of the factors, if any, that Attorney-General must consider?
b. Does this require the Attorney-General to consider potential violations of human rights?

Answer:

a. The Attorney-General must consider the Director-General's request under proposed section 34AAA(1). The Director-General's request includes analysis of the circumstances surrounding the request and would explain the basis for the request.

The Director-General's request would need to take account of the Attorney-General's Guidelines[1]. These guidelines provide for the manner in which information is to obtained by Australian Security Intelligence Organisation, namely in a lawful, timely and efficient way and in a way that is proportionate to the gravity of the threat being investigated.[2]

For completeness, we note the Attorney-General also needs to be satisfied of the matters in 34AAA(2)(c) and 34AAA(2)(d), which are as follows:

(c) the Attorney General is satisfied, on reasonable grounds, that the specified person is:
  (i) reasonably suspected of being involved in activities that are prejudicial to security; or
  (ii) the owner or lessee of the computer or device; or
  (iii) an employee of the owner or lessee of the computer or device; or
  (iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or
  (v) a person who uses or has used the computer or device; or

[1] https://www.asio.gov.au/sites/default/files/Attorney-General's%20Guidelines.pdf
[2] See specifically 10.4

(vi) a person who is or was a system administrator for the system including the computer or device; and

(d) the Attorney General is satisfied, on reasonable grounds, that the specified person has relevant knowledge of:

(i) the computer, device or a computer network of which the computer, device forms or formed a part; or

(ii) measures applied to protect data held in, or accessible from the computer or device

b. Not expressly.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 19 November 2018

HOME AFFAIRS PORTFOLIO

(*TOLA/080*) – PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY - Review of Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Schedule 5 - (Q71) - Concerns ASIO's powers under proposed section 34AAA

Asked:

71. Several submitters have raised concerns ASIO's powers under proposed section 34AAA may create the basis for the deprivation of liberty or inhumane treatment. For instance, the penalties, outlined in proposed section 34AAA(4) for a person who refuses/fails to comply with a compulsory assistance order, may have the practical effect of depriving a person's liberty for the duration of time that the person is compelled to provide assistance. This is because a person who tries to leave the premises on which assistance is sought may be taken to be refusing to comply with the compulsory assistance order–thereby committing an offence. a. What mechanisms are in place to protect the rights of persons subject to compulsory assistance orders under section 34AAA?
b. If there aren't any separate mechanisms in place, is there any reason why the power provided in this section should not be subject to the transparency and accountability mechanisms required for ASIO's questioning and detention powers?

Answer:

Section 34AAA does not provide Australian Security Intelligence Organisation with any powers of arrest or detention. In this regard it is not comparable to Australian Security Intelligence Organisation questioning and detention powers in their scope and potential to affect civil liberties. Australian Security Intelligence Organisation notes assistance orders could be issued by and conducted through, the post or by email, rendering very little intrusion or inconvenience for the specified person.

a. The offence in Section 34AAA(4) only arises where:

- the person is subject to an order under 34AAA; and
- the person is capable of complying with a requirement in the order; and
- the person omits to do an act; and
- the omission contravenes the requirement.

The fault element with respect to the offence would be recklessness.
Should the order specify a place (pursuant to 34AAA(3)(b)), Australian Security Intelligence Organisation is not empowered to restrain someone from leaving. If the person left and the leaving amounted to an omission which contravened a requirement in the order, the matter could be referred to law enforcement.

b. The computer or data storage device would be subject to a warrant or authorisation which would already be captured by the reporting requirement in Section 94(1)(a) of the *Australian Security Intelligence Organisation Act 1979*. As mentioned above – the powers in 34AAA do not grant Australian Security Intelligence Organisation powers of arrest or detention.