Australian Permanent Mission
and Consulate-General
Geneva

21 November 2018

Mr David Kaye
Special Rapporteur on the promotion and protection of the
rights to freedom of opinion and expression
Office of the High Commissioner for Human Rights
Palais des Nations
1211 Geneva 10
SWITZERLAND

Dear Sir,

Communication of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression regarding the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.

I refer to your communication, received on 11 September 2018, concerning information on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill* 2018 (the Bill) and your request for comments by the Australian Government.

As requested, the communication has been transmitted to the office of the Minister for Foreign Affairs. I am responding on the Minister's behalf.

The Australian Government acknowledges the communication and thanks you for your comments on the Bill. The proposed legislation is an important step in modernising the capacity of Australian law enforcement and security agencies to operate in the modern era, whilst maintaining due regard for cybersecurity. As your comments have dealt primarily with potential requirements on industry, this response is limited to the new industry assistance framework proposed by Schedule 1 of the Bill.

The Australian Government supports the use of communications technologies, like encryption, to protect personal privacy and sensitive information. Encryption forms a critical part of internet, computer and data security and is a cornerstone of growth and prosperity. However, the encrypt communications are being used for illicit ends and to mask online criminality. The traditional lawful surveillance powers of Australian agencies are increasingly ineffective in the digital era, a fact that jeopardies investigative outcomes and the safety of Australians.

To help key Australian law enforcement and security agencies discharge their legitimate functions, the Bill introduces a new framework through which the communications industry

can work with authorities to enforce the law and protect national security. This framework has been designed to account for a rapidly changing global environment, where communication services and devices in Australia are increasingly supplied by multiple players across the world. This framework introduces three new instruments, technical assistance requests ('requests'), technical assistance notices ('assistance notice') and technical capability notices ('capability notices') (collectively, 'notices'). The scope of and safeguards associated with each instrument is set according to the gravity of potential requirements.

Noting the importance of encryption and communications technology in promoting digital security and personal privacy, the Bill contains a number of key safeguards which are further identified below. The Government believes that this Bill represents a reasonable and proportionate means by which to address the challenges associated with the increasing prevalence of encryption.

General Concerns

Given the breadth of your comments, the Australian Government has taken care to respond to each recommendation in turn. However, before responding to your recommendations, I would like to note some safeguards in the Bill that should address some of the general concerns raised:

Decryption capabilities

You have noted that the proposed powers could require a provider to build a capability to remove electronic protection, including decrypting communications. Capability notices in proposed section 317T cannot require a capability to be built that removes electronic protection.[1] A provider may only be compelled to remove electronic protection when they have an existing capability to do so and maintain a 'decryption capability' for business purposes. To remove any doubt, proposed subsection 317ZG(2) explicitly excludes the proposed powers from being able to compel the construction of a decryption capability.

Accountability and Oversight

This Bill forms part of a broader regulatory framework that governs agency activities and surveillance powers. The comprehensive restriction in proposed section 317ZH ensures that the new powers cannot be used in replace of an existing warrant or authorisation under Australian law. This includes warrants required for communications interception or the use of surveillance devices. In most circumstances, the new powers will be used in conjunction with these underlying warrants, which are subject to judicial approval and robust independent oversight.[2]

Integrity bodies like the Inspector-General of Intelligence and Security and Commonwealth and State Ombudsman retain extensive oversight of the agencies empowered by the proposed laws, including the ability to hear complaints, conduct inspections or report on agency activities. The new Bill does not change this and the exceptions to unauthorised disclosure

[1] See 317T(4)(c)(i)

[2] See *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*

offences in section 317ZF enables information to be given to these oversight bodies if required by law.

Recommendations

Thank you for your comprehensive recommendations. While your feedback was received past the closure of the public consultation period, the concerns you raised were consistent with many responses received during consultations. The Government has responded to each in turn.

Recommendation 1 – Judicial authorisation and oversight

The new measures are designed to facilitate law enforcement and national security agencies' lawful operations as underpinned by a warrant issued by a judge or member of the Australian Administrative Appeals Tribunal. As noted above, section 317ZF prohibits the use of notices to require that a provider hand over telecommunications content and data without an underlying warrant or authorisation. Accordingly, personal information won't be gathered by these powers. Instead, they are intended to elicit technical assistance and allow agencies and industry to work collaboratively on things of a technical nature.

The Government believes that judicial oversight has limited value for technical determinations. Where significant capabilities will be developed, these must be authorised by the Attorney-General, first law officer of Australia. Ministerial authorisations for national security decisions are an established feature of the Australian legislative landscape and, for example, govern decisions to issue intelligence collection warrants or make determinations regarding the security of telecommunications systems.[3]

Providers subject to a notice retain the right of judicial review. Grounds for review may include circumstances where a technical capability notice introduces a systemic weakness into a network or where it can be shown that the decision-maker could not have considered requirements to be reasonable or proportionate. Depending on circumstances, a State court, the Federal Court or the High Court may preside over a review of the lawfulness of a decision.

The Bill also provides for both transparency reporting by providers in receipt of a technical assistance notice, technical assistance request or technical capability notice as well as mandatory annual reporting of the same notices.

Recommendation 2 –limiting the measures to significant circumstances

The Bill anchors the use of notices and requests to a 'relevant objective' which ensures these powers are only issued in serious circumstances. These objectives are consistent with the established purposes for which a broad variety of agencies can currently seek assistance from the domestic industry under section 313 of the *Telecommunications Act 1997*. These definitions are not arbitrary or unique and have been suitable to address the investigative needs of agencies to date while sufficiently limited to protect human rights. Enforcing the criminal law and national security are clear objectives which, when combined with thresholds

[3] See item 13, section 315B of the *Telecommunications and Other Legislation Amendment Act 2017*, for example.

for warranted surveillance powers, appropriately limit the purposes for which notices may be requested to serious matters.

You have raised concerns that the Bill does not explicitly require notices to meet a 'necessity' threshold. The Government considers that this threshold is met by the requirements of a decision-maker to be satisfied of the reasonableness or proportionality of the notice in proposed sections 317P and 317V. While considerations of reasonableness and proportionality inherently go to the need of any requirements set, to remove doubt changes were made following public consultation to require a decision-maker to consider 'the availability of other means to achieve the objectives of the notice'.[4]

Recommendation 3 – A clear and acceptable definition for 'systemic weakness' should be provided

While the Bill does not provide a definition of 'systemic weakness', provisions have been included to ensure notices cannot be used to require a provider to implement or build flaws into their services or devices that would jeopardise the security of innocent, third-parties. Proposed section 317ZG prevents a weakness or vulnerability from being built into a single item (like a target service or device) if it would undermine the security of other, interconnected items. That is, where the weakness in one part of the system would compromise other parts of the system or the system itself, such a measure is impermissible. The term 'systemic' does not include weaknesses or vulnerabilities that could be isolated to a particular device (access to which would be subject to an underlying warrant). Rather, the provision prohibits notices that impact forms of electronic protection on non-target services and devices.

The prohibition in proposed section 317ZG is complimented by two key limitations in both the assistance notice and capability notice provisions. Assistance notices cannot require a provider to do a thing they are not already capable of doing, therefore its potential to implement systemic weaknesses in a system is limited by the fact that these weaknesses would likely need to be created by a new capability. A capability notice cannot require the construction of a capability to remove a form of electronic protection and is thus limited in any requirements it may impose that cause flaws in forms of electronic protection.

Following consultations, a new provision was introduced (proposed subsections 317W(7) – (11)) to allow the Attorney-General and a provider to jointly appoint a person with technical expertise to undertake an assessment of whether the requirements in a technical capability notice would contravene proposed section 317ZG. The intent of the change was to facilitate scrutiny by the technical community whilst appropriately protecting sensitive law enforcement and national security capabilities as well as sensitive commercial information. In any case, if a provider believes that a notice would contravene proposed section 317G they may refer the decision for judicial review which would provide an opportunity for expert evidence to be tendered regarding the cybersecurity implications of compliance.

Leaving 'systemic weakness' undefined is an acknowledgement that IT systems are not identical. What amounts to a 'systemic weakness' in one system may not in another. In this way provision in section 317ZG gives providers the opportunity to identify systemic weaknesses in notices issued to them without the burden of meeting a prescriptive standard,

[4] See proposed sections 317RA(e) and 317ZAA(e).

which, in a technically complex and evolving industry, could lead to legislative loopholes. Because of their knowledge of their computer systems, providers are best-placed to determine if a proposed modification amounts to a 'systemic weakness'.

Recommendation 4 – Prohibiting the storage of all user data or the establishment of key escrows

The intent of this legislation is not to introduce forms of exceptional access like key escrow or require easier access to communications via data localisation laws. Proposed subsection 317ZG sets out that neither a notice can be used to establish a regime of key escrows where this would amount to the implementation of a new decryption capability in electronic protection or the creation of a systemic weakness. Forcing a provider to redesign their system to introduce a key escrow scheme or localise data, which would potentially introduce further points of access for malicious actors, would need to meet the strict prohibitions in the legislation including the standards of reasonableness, practicality, technical feasibility and proportionality.

Recommendation 5 – Reduction of penalties for non-compliance with Schedule 1

The civil penalties set out in proposed section 317ZB for failing to comply with a notice are consistent with the rationale for enforcement elsewhere in the Telecommunications Act and equivalent to the penalties for carriers and carriage service providers for breach of a carrier licence in Part 31 of the Telecommunications Act.

The penalty units in proposed section 317ZB are calculated to achieve deterrence and are set proportionally to the limits of seriousness for contravention. The broad range of entities that may be subject to requirements in a notice requires a higher maximum penalty. The supply of communications services and devices can be a highly profitable enterprise. Most of the providers that may be impacted by the new powers have significant financial reserves. Lower maximum penalties would be unlikely to achieve deterrence.

The penalty amounts also reflect the significant loss that may result from non-compliance with a notice. Failure to act in good faith with any requirements may jeopardise ongoing criminal investigations, result in the destruction of material evidence or, in extreme cases, expose the Australian public to serious harm.

Recommendation 6 – Ongoing consultation with civil society, corporations and general public

The Government has conducted significant consultation on the entire Bill amongst Government, industry, civil society groups and the public. Consultations can be divided into three distinct stages:

- Preliminary industry consultations (July 2017 – June 2018)
- Targeted industry consultations (28 June 2018 – 14 August 2018)
- Public consultations (14 August 2018 - 10 September 2018)

Significant changes have been made to the Bill on the basis of feedback received in both industry consultations and public consultations. These changes address key concerns raised and reinforce the policy intent of the Bill. Key changes to the Bill include:

- requiring decision-makers to consider set matters, including privacy and cybersecurity, when deciding whether a notice is 'reasonable and proportionate'
- establishing a mechanism for independent, technical review, of the effect of requirements in a capability notice
- requiring decision-makers to explain to a provider their obligations under a request or notice
- strengthening the limitation that prevents notices from being issued in substitution of an existing warrant or authorisation
- establishing a defence for providers where there may be a conflict of laws

All submissions received during the consultation period with consent to publish have been made available on the Department of Home Affairs website and can be viewed at: https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018 The Government appreciates the thorough feedback on the exposure draft of the Bill.

As you may be aware, this Bill was introduced into the Australian Parliament on 20 September 2018 by the Minister for Home Affairs, the Hon Peter Dutton MP. It has since been referred to the Parliamentary Joint Committee on Intelligence and Security for further scrutiny and review.

The Australian Government is committed to maintaining the integrity of encryption and other forms of electronic protection that are vital to prosperity in the digital age. The measures in this Bill will ensure that requirements placed on persons integral to the supply of communications in Australia are reasonable and proportionate means to ensuring the safety of the public and enable authorities to undertake lawful, warranted and targeted surveillance without undermining the security of communications.

I trust the above information will be of assistance to you in clarifying the concerns conveyed in the communication. I look forward to your continued engagement with the Australian Government's efforts to protect the rights of individuals in Australia.

Yours sincerely

S. Mansfield.

Sally Mansfield
Ambassador and Permanent Representative