FROM THE PERMANENT REPRESENTATIVE

AUSTRALIAN PERMANENT MISSION

GENEVA

1 April 2019

Mr. Joseph Cannataci
Special Rapporteur on the right to privacy
United Nations Office at Geneva
8-14, avenue de la Paix
1211 Geneva 10, Switzerland

e-mail: registry@ohchr.org

Dear Special Rapporteur,

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Thank you for your comments on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill). The Bill passed both houses of Parliament on 6 December 2018 and received royal assent on 8 December 2018.

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act) 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.

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 digital prosperity. However, the evolving digital environment, including the growing use of encrypted technologies by terrorists and criminals, presents an increasing challenge for law enforcement and national security agencies. The impact of encryption is clear:

- Over 90 per cent of data being lawfully intercepted by the Australian Federal Police now uses some form of encryption.
- Encryption impacts at least nine out of every ten of the Australian Security Intelligence Organisation's priority cases.
- Australian Border Force activities to disrupt and deter organised criminal activities, such as the importation of drugs and pre-cursor chemicals, often encounter sophisticated methodologies using Information Communications Technology.

Law enforcement and national security agencies have the ability to seize devices and access communications such as text messages, provided there is a warrant issued by a judge or similar independent authority. However, gaining valuable and intelligible information through traditional interception methods is increasingly difficult due to the prevalence of encryption and the rapid evolution of modern communications technology. In most instances encryption is incapable of being overcome, limiting the possible avenues for investigation and perpetuating serious threats to the public. In other instances, law enforcement agencies may have to employ expensive and time-consuming techniques to unlock a device or read encrypted communications. Not only does this increase the cost of operations, the delay it introduces can substantially raise the risk of harm or loss of life. The inability of agencies to read lawfully obtained communications has a significant impact on public safety and national security.

To help key Australian law enforcement and security agencies discharge their legitimate functions, the Act 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 are increasingly supplied by multiple entities across the world. This framework introduces three new instruments; technical assistance requests (TARs or requests), technical assistance notices (TANs) and technical capability notices (TCNs) (collectively, 'notices'). The scope of, and safeguards associated with, each instrument is set according to the gravity of potential requirements.

Given the importance of encryption and communications technology in promoting digital security and personal privacy, the Act contains a number of key safeguards which are identified below. The Government believes that this Act represents a reasonable and proportionate means by which to address the challenges associated with the increasing prevalence of encryption. These strong safeguards ensure that the privacy of Australians is not compromised and that assistance rendered does not jeopardise the security of the digital ecosystem.

Since receipt of your letter on 12 October 2018, significant amendments have been made to the legislation. These amendments reflect the outcome of consultation on the exposure draft of the Bill, and Parliamentary reviews from the Parliamentary Joint Committee on Intelligence and Security, Parliamentary Joint Committee on Human Rights and Senate Standing Committee for the Scrutiny of Bills. As the legislation has been enacted, and your comments relate to an exposure draft of the Bill, this letter will detail important amendments moved in Parliament to strengthen those measures related to privacy.

Amendments in relation to privacy matters

The Act contains a number of amendments that increase transparency, and strengthen the existing accountability and oversight measures. This ensures that the powers in the Act are only used when required to facilitate our law enforcement and national security agencies' legitimate and lawful operations.

Amendments were also made to strengthen existing legislative limitations, which seek to ensure key measures do not arbitrarily or unlawfully interfere with a person's privacy under Article 17 of the *International Covenant on Civil and Political* Rights (ICCPR), while equipping law enforcement and national security agencies with the tools to investigate and prosecute serious criminal and terrorist activities. These amendments:

- Establish definitions of 'serious Australian offence' and 'serious foreign offence' to limit the scope of the industry assistance framework introduced into new Part 15 of the *Telecommunications Act 1997* (Telecommunications Act), through Schedule 1 of the Assistance and Access Act. Limiting the scope of industry assistance to 'serious Australian offence' and 'serious foreign offence' ensures the powers set out in new Part 15 (the industry assistance measures) can only be exercised in relation to a law that is punishable by a maximum term of imprisonment of 3 years or more, or for life. These definitions ensure that the issuing of a TAR, TAN or TCN is reserved for serious offences including terrorism and child exploitation offences. Invoking the powers in Part 15 is a reasonable, necessary and proportionate limitation of the prohibition on interference with privacy given the nature of the offences under investigation.
- Require decision-makers under the Telecommunications Act to consider if the form of industry assistance required under a TAN or TCN is the least intrusive known form of industry assistance available in relation to the impact on the privacy of innocent third parties

(section 317JC for TARs, section 317RA for TANs and new section 317ZAA for TCNs). This requirement to assess whether the proposed industry assistance is the least intrusive minimises the risk of new Part 15 powers being used arbitrarily to interfere with the privacy of innocent parties.

- Strengthen decision-making criteria for the issuing of a compulsory industry assistance notice under Part 15 to ensure providers will not be asked to do anything that will make their networks or devices less secure or place the privacy of persons at risk.

  Section 317P of the Telecommunications Act ensures that TANs can only be issued if the decision-maker is satisfied that the requirements imposed by the notice are reasonable and proportionate, and that compliance with the notice is practicable and technically feasible. A TAN itself is restricted to compelling assistance that is within the existing business capacity of a provider. Similarly, section 317V in the Telecommunications Act ensures that TCNs can only be issued if the Attorney-General is satisfied that the requirements imposed by the notice are reasonable and proportionate, and that compliance with a notice is practicable and technically feasible. Under section 317JAA, decision-makers are now required to consider the same factors before issuing a TAR.

  New sections 317JC, 317RA and 317ZAA of the Telecommunications Act include considerations of necessity, amongst other things, which strengthens the aforementioned decision-making criteria to require decisions-makers have regard to whether a TAR, TAN or TCN is necessary for achieving legitimate beneficial outcomes for law enforcement and national security.

  New sections 317JC, 317RA and 317ZAA provide confidence that, under the oversight of the decision-maker, any limitation on a person's privacy arising from a compulsory notice issued under new Part 15 of the Telecommunications Act is permissible as being necessary to ensure national security and public order. The new provisions require the decision-maker to have regard to, among other factors, national security or law enforcement matters, whether the request is necessary and the least intrusive form of industry assistance, and the legitimate expectations of the Australian community relating to privacy and cyber security.

- Impose a 12 month time-limit on TANs and TCNs in new sections 317MA and 317TA in the Telecommunications Act. This mandatory time-limit (extendable for a period of a further 12 months with the agreement of the provider) ensures notices are not in perpetuate existence and that decision-makers re-evaluate the necessity, reasonableness and proportionality of a notice if it is required for more than 12 months.

- Extend the consultation requirements to all the compulsory powers in new Part 15 (TANs and TCNs). Section 317W requires the Attorney-General to consult with the impacted provider prior to issuing a TCN. The Government amendments introduced new section 317PA of the Telecommunications Act which requires the decision-maker to consult with the provider prior to the issuing of a TAN. These mandatory consultations will ensure Government and industry can reach mutually agreeable terms for assistance rendered and ensure, for example, that any impost is minimal and does not impact cyber security. If the provider voluntarily notifies the relevant agency, in a form they deem to be appropriate, of their decision to waive the right to be consulted, then consultation requirements will not apply.

The purpose of this provision is to give certainty to providers that requirements in a notice have been issued with due regard to their legitimate concerns, as is required in the decision-making criteria. It also legislates the steps agencies must undertake when determining the requirements in a notice. This amendment is supported by other consultative measures in the Act including the requirement for notices to be provided in writing to the provider under section 317M of the Telecommunications Act.

By giving the provider an opportunity to raise any concerns associated with the proposed notice, this amendment seeks to ensure that the compulsory powers in Part 15 are not exercised arbitrarily, and ensures that the decision-maker is made aware of, and can consider, any unintended consequences that may result from the issuing of a notice under Part 15.

- New section 317MAA, requires decision-makers to notify the provider of their right to complain about an agencies' activities to the relevant Commonwealth, State or Territory oversight body, ensuring that they have a clear avenue for redress.
- Create an exhaustive list of 'listed acts and things' in section 317E of the Telecommunications Act for TANs and TCNs. In other words, TANs and TCNs can only be issued in respect to those listed acts or things in section 317E. Prior to this amendment, TANs could be issued for matters that were determined by the decision-maker to meet criteria in section 317P of the Telecommunications Act and, while consistent with 317E, were not directly provided for in the listed acts or things.

  The listed acts or things are necessary to ensure agencies can continue to discharge their functions which are critical to maintaining national security and public order. This exhaustive list provides further clarity as to the situations that permit the use of Schedule 1 powers which seeks to ensure that notices are not issued arbitrarily.

Clarifying the intent, and strengthening the operation of section 317ZG

The amendments introduced additional safeguards into section 317ZG to strengthen the prohibition against providers being required to implement or build a systemic weakness or vulnerability into a form of electronic protection. The prohibition in section 317ZG includes actions which would make systemic methods of authentication or encryption less effective and explicitly prohibits requiring a provider to construct a decryption capability. The amended legislation extends this prohibition to TANs and TARs. The amendments also introduce a robust independent assessment process, which can be instigated by the provider, to determine the ultimate security implications, intrusiveness and reasonableness, of any capability the provider is required to develop.

New subsections 317ZG(4A) to (4C) also limit the interferences with privacy in Part 15 by ensuring the security of third party communications are not impacted. Specifically, this section assists in preventing requests and notices from being used as vehicles to introduce systemic weaknesses and vulnerabilities which can fundamentally undermine the security of networks and devices. The amendments enhance the operation of new section 317ZG by clarifying that where agencies undertake activities to target a particular service or device, that activity must not jeopardise the information security of any other person. The term 'jeopardise the security of information' explicitly includes an act or thing that would create a material risk that otherwise secure information can be accessed by an unauthorised third party. This further strengthens provisions that prevent the powers in Part 15 from being used to interfere arbitrarily or unlawfully with the privacy of innocent parties.

Particular amendments related to section 317ZG include:

- Introducing a definition for 'systemic weakness' and 'systemic vulnerability' in new section 317B. The definition clarifies and prohibits proposed requirements in a notice or request that would create an unacceptable risk that assistance rendered would jeopardise the information security of 'innocent parties'. This definition makes clear that anything which weakens whole systems (including sub-systems within items of technology), and consequently puts the security of innocent users at risk, is prohibited. The definition establishes a carve-out for the targeted use of the powers where the use can be isolated to particular device or service and does not create a broader risk to system security.

- Introducing a non-exhaustive definition of 'electronic protection' in new section 317B to clearly anchor the prohibition against systemic weaknesses to key cyber security technologies like encryption and authentication (password) technologies.

- Introducing a definition of 'target technology' in new section 317B to clarify the targeted use of the powers. This ensures that the powers in Part 15 can only be used in respect of a specific device or network connected to a particular person.

- Introducing new section 317WA in the Telecommunications Act which establishes a framework for providers to request the carrying out of an assessment of a TCN. The independent assessors appointed under subsection 317WA(2) will consider whether a requirement to build a new capability would create a systemic weakness and whether it is reasonable, proportionate, practicable and technically feasible to do so and provide a report. The Attorney-General must consider the report when issuing a notice.

  The independent assessors are persons eminently qualified to scrutinise the security implications of new capabilities, one being a person with cyber security or other relevant technical expertise, and the other a retired senior judge. The technical expert will be appointed for their particular subject matter experience and will assist the judicial assessor in understanding the necessary technical dimensions of the capability. As a former senior judge, the judicial assessor will be a person of integrity with demonstrated legal acumen and public service. These qualities ensure they are well-placed to determine legal thresholds of reasonableness and proportionality. These experts will assess whether:

  - the requirements imposed by the notice are reasonable and proportionate,
  - compliance with the notice is practicable and technically feasible, and
  - the notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice.

  This is an additional safeguard to the consultation requirements under section 317W. The purpose of this amendment is to ensure providers are afforded an opportunity to challenge the requirements in a notice if they believe it may lead to the introduction of a systemic weakness or vulnerability or if the requirements are not reasonable or proportionate. This is an important measure as it ensures that the requirements in a proposed notice are altered before the notice is issued in order to prevent those systems which maintain the security of personal information from being undermined.

New section 317ZG is an important safeguard that supports Part 15 and ensures that the related powers are not an unlawful or arbitrary interference with a person's privacy and to the extent the

prohibition is limited, the amendments ensure that the limitations are necessary, reasonable and proportionate to ensure effective law enforcement and national security.

Enhanced approval, inspection and oversight

The amendments establish a process whereby TCNs require joint authorisation from both the Attorney-General and Minister for Communications. This will ensure that TCNs will only be issued when an appropriately high level of authorisation and scrutiny has been applied to a relevant request and requires explicit consideration of industry interests by the Minister for Communications. Given the gravity of TCNs, this 'double-lock' approval process provides an opportunity for the communications industry to raise broader concerns with the use of these powers and maintains the proprietary of notices. This process is complimented by the new provisions that allow for independent assessment of a notices' requirements.

Further, the amendments include a suite of enhanced oversight measures, including robust notification requirements and clear authority for the Inspector-General of Intelligence and Security (IGIS), Commonwealth Ombudsman and State and Territory oversight bodies to inspect and report on the use of powers under the Act.

Existing reporting regimes have been augmented to allow the Commonwealth Ombudsman to further scrutinise the use of industry assistance measures in conjunction with underlying interception and surveillance powers. Further, the Act now establishes clear channels for information exchange between oversight bodies to ensure the necessary information is available to State and Territory oversight bodies when they are assessing agency compliance with the law.

Reporting requirements have been set for powers across the Act, including in classified Australian Security Intelligence Organisation (ASIO) annual reports that are scrutinised by Parliament and Government.

Additional protections Schedules 2 & 5

Additional restrictions, reporting and notification measures have been placed on the exercise of computer access powers by law enforcement and ASIO and also on compulsory orders to aid access to data by the Attorney-General. These amendments, in Schedules 2 and 5 of the Act, further limit the use of intrusive and covert powers and allow oversight bodies to better monitor their exercise.

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 the Act will ensure that requirements placed on providers are reasonable, necessary and proportionate means to ensuring the legitimate aim of securing the safety of the public and enabling agencies to undertake lawful, warranted and targeted surveillance without undermining the security of communications.

Thank you for your engagement and the opportunity to respond to your concerns.

Sally Mansfield.

Sally Mansfield
Ambassador and Permanent Representative
Australian Permanent Mission to the United Nations
Australian Delegation to the Conference on Disarmament