Australian Government
Office of the Australian Information Commissioner

Our reference: D2018/012308

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

By email: pjcis@aph.gov.au

Submission to the Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Dear Mr Hastie

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill) and explanatory memorandum.

1. The *Privacy Act 1988* (Privacy Act) confers on the Australian Information Commissioner and Privacy Commissioner (the Commissioner) a range of privacy regulatory functions and powers. A function of the Commissioner is to examine a proposed enactment that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals.[3] The Commissioner also has the function of ensuring that any adverse effects of the proposed enactment on the privacy of individuals are minimised.[4] In performing functions, the Commissioner must have due regard to the objects of the Privacy Act.

2. The objects of the Privacy Act include to 'promote the protection of the privacy of individuals,' to 'recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities,' to 'promote responsible and transparent handling of personal information by entities,' to 'facilitate the free flow of information across borders while ensuring that the privacy of individuals is respected,' and to 'implement Australia's international obligations in relation to privacy.'[5]

[3] Section 28(2)(a) of the Privacy Act.

[4] Section 28(2)(c) of the Privacy Act.

[5] Section 2A(a), (b), (d), (f) and (h) of the Privacy Act.

3. A central principle in the Privacy Act is the protection of personal information—regulated entities must take reasonable steps to protect the security of personal information[6] and must notify individuals and the OAIC in the event of a serious data breach.[7] These are important obligations which seek to safeguard the security of individuals' personal information held by regulated organisations and agencies. If passed, the Bill would invoke exceptions to the Australian Privacy Principles (APPs), and permit an interference with privacy where acts or practices are required or authorised by or under an Australian law, or a court/tribunal order.

4. While Australia's privacy laws recognise that the protection of individuals' privacy is not an absolute right, any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.[8] For new law enforcement initiatives that adversely impact privacy, this includes demonstrating the necessity of the proposal through evidence, and ensuring that the scope of proposed measures is as clear and transparent as possible. Where an adverse impact on privacy is necessary, a commensurate increase in oversight, accountability and transparency is required, to strike an appropriate balance between any privacy impacts and law enforcement and national security objectives.

5. The Bill would introduce a number of new powers intended to assist intelligence and law enforcement agencies in responding to the current technological environment, and in particular to the increased use of encrypted communications.[9] These include new powers in Schedule 1 to issue technical assistance requests (TARs),[10] technical assistance notices (TANs),[11] and technical capability notices (TCNs).[12] The OAIC acknowledges that the power to issue TANs and TCNs is subject to certain limitations, including that a TAN or TCN must not have the effect of requiring a systemic weakness or vulnerability to be built into a form of electronic protection.[13] However, it will be necessary to ensure that the measures proposed in Schedule 1 do not, in practice, introduce unintended exploitable weaknesses into a telecommunications environment that fundamentally relies on strong and robust security settings.

---

[6] Australian Privacy Principle 11, Schedule 1 of the Privacy Act.

[7] Part IIIC of the Privacy Act. Entities with security obligations under the Privacy Act are required to notify individuals and the OAIC of an 'eligible' data breach. A data breach is 'eligible' if it is likely to result in serious harm to any of the individuals to whom the information relates. More information on eligible data breaches is available on the OAIC's website at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches>.

[8] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), paragraph 23, <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>.

[9] Explanatory memorandum, pg. 1-2.

[10] Section 317G in Schedule 1 of the Bill.

[11] Section 317L in Schedule 1 of the Bill.

[12] Section 317T in Schedule 1 of the Bill.

[13] Section 317ZG in Schedule 1 of the Bill.

6. The OAIC welcomed the opportunity to make a submission to the Department of Home Affairs in September 2018, in relation to its public consultation on the draft Assistance and Access Bill 2018.[16] While the OAIC acknowledges that the Bill and explanatory memorandum before the Committee addresses some of the recommendations in the OAIC's earlier submission, privacy risks remain.

7. The OAIC's submission to the Committee focuses on Schedule 1 of the Bill and makes 10 recommendations. The OAIC recommends that Schedule 1 of the Bill:

   a. define the terms 'systemic weakness' and 'systemic vulnerability' in s 317ZG

   b. extend s 317ZG, which provides that a TAN or TCN must not require a designated provider to implement or build a 'systemic weakness' or a 'systemic vulnerability' into a form of electronic protection, to TARs

   c. clarify the obligations on a designated provider and the issuer of the TAR, TAN or TCN to determine a notice's compliance with s 317ZG, and whether a designated provider's reasonable belief that a notice does not comply with s 317ZG is a defence to the enforcement provisions in Division 5

   d. require prior technical assessment of all TARs, TANs and TCNs, before they are issued, to confirm that the 'acts or things' listed in them do not have any unintended effects on security systems

   e. include an exhaustive list of all 'acts or things' in s 317E (rather than use discretionary powers or rules) for all TARs, TANs and TCNs, and that if additional types of 'acts or things' need to be added, amendments could be made to the primary legislation. Alternatively, if that recommendation is not accepted, the rule-making power in s 317T(5) applying to TCNs, should extend to TARs and TANs, and should include privacy as a matter that must be considered

   f. require judicial oversight of a proposed notice, before a TAR, TAN or TCN is issued, and provide for technical expertise to be considered during this process

   g. extend the decision-making criteria of reasonableness, proportionality, practicability and technical feasibility to TARs, including that privacy impacts be considered when assessing whether a TAR is reasonable and proportionate

   h. require consideration of whether a warrant is already in place for accessing particular content, when assessing whether a TAN or TCN is reasonable and proportionate

[16] <https://www.oaic.gov.au/engage-with-us/submissions/public-consultation-on-the-telecommunications-and-other-legislation-amendment-assistance-and-access-bill-2018-submission-to-department-of-home-affairs>

i. broaden the annual statistics reporting requirements in s 317ZS

j. include a sunset clause, or alternatively, provide a designated time for review of the framework.

The role of the OAIC and the Privacy Act 1988

8. The OAIC has regulatory oversight of the Privacy Act, which outlines how Australian Privacy Principle (APP) entities (including most Australian Government agencies, and all private sector and not-for-profit organisations with an annual turnover of more than $3 million), must handle, use and manage individuals' personal information.

9. While the Privacy Act generally applies to the Australian Federal Police and to designated communications providers (designated providers)[17] that are also APP entities, it does not apply to the Australian Secret Intelligence Organisation, the Australian Secret Intelligence Service or the Australian Signals Directorate[18] or to State or Territory agencies such as police forces. Additionally, the Privacy Act would generally not apply to designated providers with an annual turnover of less than $3 million.[19]

10. The Privacy Act includes 13 legally binding APPs. The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information. For example, APP 6 requires entities to only use or disclose personal information for the purpose for which it was collected, unless the individual has consented or an exception applies.[20] APP 11 requires APP entities to take reasonable steps to protect personal information they hold, from misuse, interference, loss, unauthorised access, modification or disclosure.

11. As noted in the OAIC's *Guide to Securing Personal Information*, encryption is an important mechanism that APP entities can use to satisfy their APP 11 requirements.[21] Further, in the event of a data breach, entities with security obligations under the Privacy Act are required to comply with the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act. The fact that personal information is encrypted may reduce the likelihood of serious harm in

---

[17] Section 317C in Schedule 1 of the Bill.

[18] Section 7(1) of the Privacy Act. The Privacy Act also exempts disclosures of personal information to these intelligence agencies: s 7(1A).

[19] Section 6D of the Privacy Act. Section 187LA of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) provides that the Privacy Act applies to all service providers (including small business operators with an annual turnover of less than $3 million) to the extent that the activities of the service provider relate to data retained under Part 5-1A of the TIA Act.

[20] Exceptions include where a use or disclosure is required or authorized by law (APP 6.2(a)), and where a use or disclosure is reasonably necessary for a law enforcement activity conducted by an enforcement body (APP 6.2(e)).

[21] <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>

the event of a data breach and therefore avoid the requirement to notify the OAIC or affected individuals.[22]

12. If passed, the Bill would invoke exceptions to the APPs, where acts or practices are required or authorised by or under an Australian law, or court/tribunal order.

Scope and application of TARs, TANs and TCNs

13. The OAIC welcomes the intent of s 317ZG in Schedule 1 of the Bill, which provides that a TAN or TCN must not require a designated provider to implement or build a 'systemic weakness' or a 'systemic vulnerability' into a form of electronic protection.[23] This includes limitations on:

- requiring the implementation or building of a new decryption capability[24]
- requiring one or more actions that would render systemic methods of authentication or encryption less effective.[25]

14. In addition, a TAN or TCN must not prevent a designated provider from rectifying a systemic weakness or a systemic vulnerability in a form of electronic protection.[26]

15. These limitations may provide an important safeguard – given the fundamental reliance on robust security practices to support Australians' day-to-day communications. However, it will be necessary to ensure that, in practice, measures proposed in Schedule 1 do not result in an unintended weakening of security systems, or increase the potential for a data breach. To minimise this risk, the scope of the measures in Schedule 1 should be clear and transparent, to enable an evaluation of whether these are reasonable, necessary and proportionate in the circumstances.

'Systemic weakness' and 'systemic vulnerability'

16. The OAIC recommends that the Bill define the terms 'systemic weakness' and 'systemic vulnerability' in s 317ZG. The OAIC considers that the explanation of these terms in the explanatory memorandum, that 'the nature and scope of any weakness and vulnerability will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required',[27] does not make the intended scope of this exception clear. In addition, while the explanatory memorandum provides an example of access to

---

[22] For more information about how encryption may affect whether there is a risk of serious harm to an individual, see the OAIC's *Data Breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*, available at <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>.

[23] Section 317ZG(1) in Schedule 1 of the Bill.

[24] Sections 317ZG(2) in Schedule 1 of the Bill.

[25] Sections 317ZG(3) in Schedule 1 of the Bill.

[26] Section 317ZG(4) in Schedule 1 of the Bill.

[27] Explanatory memorandum, paragraph 258.

encrypted information on a particular device that may not result in a systemic weakness,[28] a single example may be of limited assistance for designated providers in determining whether the nature and scope of any weakness or vulnerability amounts to a systemic weakness. As such, designated providers that receive a TAN or TCN may be uncertain about how this important privacy safeguard applies in practice to their particular situation. It is also more difficult to evaluate the scope of this safeguard, and whether any privacy impacts of issuing a TAN or TCN are reasonable, necessary and proportionate in the circumstances.

17. In defining these terms, the OAIC recommends that the Bill be amended to ensure that steps taken by designated providers in response to a TAN or TCN do not enable broader misuse, interference, loss, or unauthorised access, modification or disclosure, of personal information.[29] For example, the definition could ensure that there is no weakening of security systems affecting any individuals that are not involved in a current investigation. The OAIC also suggests including some further practical examples of systemic and non-systemic weaknesses and vulnerabilities in the explanatory memorandum to clarify the scope of this safeguard.

18. The OAIC notes that the limitation in s 317ZG does not extend to a TAR. As noted in the explanatory memorandum, the limitation that s 317ZG imposes on TANs and TCNs 'protects the fundamental security of software and devices', and ensures that 'the products Australians enjoy and rely on cannot be made vulnerable to interference by malicious actors'.[30] These policy considerations appear to apply equally to voluntary notices. The OAIC therefore recommends that s 317ZG be extended to apply to TARs, on the basis that it cannot be assumed that all designated providers will not comply with a TAR, even when they have concerns about introducing systemic weaknesses and vulnerabilities. Extending s 317ZG in this way may be particularly important for customers of small designated providers that may not have the resource capacity to assess whether a TAR may introduce systemic weaknesses or vulnerabilities.

19. The OAIC also recommends that the Bill clarify the obligations on a designated provider and the issuer of a TAR, TAN or TCN to determine a notice's compliance with s 317ZG. The Bill should also clarify whether a designated provider's reasonable belief that a notice does not comply with s 317ZG is a defence to the enforcement provisions in Division 5.

---

[28] See the explanatory memorandum, which provides the following example: 'if any agency were undertaking an investigation into an act of terrorism and a provider was capable of removing encryption from the device of a terrorism suspect without weakening other devices in the market then the provider could be compelled under a technical assistance notice to provide help to the agency by removing the electronic protection. The mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built.' (paragraph 258).

[29] APP 11 in the Privacy Act requires APP entities to take reasonable steps to protect personal information they hold, from misuse, interference, loss, unauthorised access, modification or disclosure.

[30] Explanatory memorandum, paragraph 256.

Technical assessment

20. The OAIC considers that the Bill should ensure that weaknesses and vulnerabilities are not unintentionally created because the impact of a particular request is not fully understood by the agency or the designated service provider.

21. In this regard, the OAIC welcomes the addition, since public consultation on the draft Bill, of ss 317W(7)-(11), the effect of which is that during the consultation period for a TCN, the Attorney-General and a designated provider may jointly appoint one or more persons to carry out an assessment of whether a proposed TCN would contravene the systemic weakness limitation in s 317ZG.

22. In the OAIC's view, however, a mandatory technical assessment of all TARs, TANs and TCNs before they are issued, would better meet the objectives of s 317ZG. This would help to confirm that the 'acts or things' listed in a TAR, TAN or TCN do not have any unintended effects on security systems.[31] It may also enhance public confidence that the issuing of a request or notice will not result in an unintended weakening of security systems, regardless of the designated provider's commercial interests (which might not always align with the public interest), and capacity to pay. Technical assessments could also be taken into consideration as part of the 'judicial oversight' mechanisms recommended below.

Defined 'acts or things' in s 317E

23. Section 317E includes a non-exhaustive list of 'acts or things' that may be included in a TAR or a TAN.[32] This appears to confer a broad discretionary power for a decision-maker to determine the kind of assistance that is appropriate in the circumstances. In addition, the range of acts or things that may be specified in a TCN can be expanded by legislative instrument.[33] While the OAIC recognises that in some circumstances it is necessary to provide for flexibility through discretionary powers, limitations on transparency make it difficult to fully assess the privacy impacts of any proposed information handling practices.[34] They also limit external scrutiny of these measures, particularly given the secrecy provisions that prohibit unauthorised disclosure of information about TARs, TANs and TCNs under s 317ZF.

24. The OAIC recommends that s 317E include an exhaustive list of all 'acts or things' (rather than use discretionary powers or rules) for TARs, TANs and TCNs. If additional types of 'acts or things' need to be added over time, the primary legislation could be amended,

---

[31] This point, that new systems and features should be tested before use, is generally made by the authors of *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* (2015), available at <https://dspace.mit.edu/handle/1721.1/97690>.

[32] Sections 317G(6), 317L(3), respectively in Schedule 1 of the Bill.

[33] Sections 317T(4)(c)(ii), (5) in Schedule 1 of the Bill.

[34] The importance of open and transparent management of personal information to individuals' expectations of privacy is reflected in the objects of the Privacy Act, which includes promoting 'responsible and transparent handling of personal information by entities' (see section 2A of the Privacy Act).

necessitating greater Parliamentary oversight. Alternatively, if this is not accepted, the OAIC recommends that the model used for TCNs is applied to TARs and TANs. That is, an exhaustive list accompanied by a rule-making power. If a rule-making power were to be included in Schedule 1, the OAIC recommends including obligations in the primary legislation to ensure that privacy is given appropriate consideration in the making of the rules.

Oversight and accountability

25. Schedule 1 in the Bill facilitates access by intelligence and interception agencies to encrypted communications, in circumstances where individuals may otherwise have an expectation that such communications are private. In the OAIC's view, new law enforcement initiatives that impact on privacy require a commensurate increase in oversight, accountability and transparency, to strike an appropriate balance between any privacy intrusions and law enforcement and national security objectives.

26. In this regard, the OAIC acknowledges the current safeguards and oversight measures in the Bill, including annual reporting requirements,[35] Ministerial oversight for the issuing of TCNs[36] and a requirement that the senior decision-maker be satisfied that requirements in a TAN or TCN are reasonable, proportionate, practicable and technically feasible[37] (including a requirement to consider the 'legitimate expectations of the Australian community relating to privacy and cybersecurity' when assessing whether the requirements imposed by a TAN or TCN and 'reasonable and proportionate').[38] In addition, TANs and TCNs cannot be used to circumvent the existing warrant process, if a warrant is required to access private communications or data.[39]

27. The OAIC makes recommendations for additional oversight and accountability mechanisms below.

Judicial oversight

28. The OAIC understands that decisions made under Schedule 1 to issue a TAR, TAN or TCN will be decisions to which the *Administrative Decisions (Judicial Review) Act 1997* does not apply. Judicial review will be available through the original jurisdiction of the High Court, or through the Federal Court of Australia by operation of s 39B(1) of *the Judiciary Act 1903*, to ensure that decisions are made within the legal limits of the relevant powers.[40]

---

[35] Section 317ZS in Schedule 1 of the Bill.

[36] Section 317T(1) in Schedule 1 of the Bill.

[37] Section 317P and 317V in Schedule 1 of the Bill.

[38] Section 317RA and 317ZAA in Schedule 1 of the Bill.

[39] Section 317ZH and p. 68 of the explanatory memorandum.

[40] See the new paragraph (daaaa) in Schedule 1 of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) that is to be inserted as part of Schedule 1 of the draft Bill. See also paragraphs 7 and 8 of the explanatory memorandum.

29. The OAIC notes that similar assistance and access powers under the UK's *Investigatory Powers Act 2016* (IPA) provide for independent review of decisions made to issue a technical capability notice. Under the IPA, the Secretary of State may only give a relevant operator a technical capability notice if the decision to give the notice has been approved by a Judicial Commissioner. In deciding whether to approve a decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions with regard to whether 'the notice is necessary', and whether 'the conduct required by the notice is proportionate to what is sought to be achieved by that conduct'.[41] When assessing proportionality, the Judicial Commissioner must have regard to the general duties in relation to privacy that are set out in section 2 of the IPA.

30. The OAIC recommends including in Schedule 1 judicial oversight mechanisms similar to those in the UK model, to provide for an additional evaluation as to whether each notice is necessary and proportionate before it is issued. These oversight mechanisms should also consider the findings of the prior technical assessment.

Requirement to consider impacts on privacy

31. As noted above, ss 317P and 317V in Schedule 1 require a decision-maker to consider whether the requirements imposed by a TAN or TCN are reasonable and proportionate, and whether compliance with the TAN or TCN is practicable and technically feasible. The OAIC welcomes that ss 317RA and 317ZAA have been inserted since public consultation, to provide further detail about relevant considerations under ss 317P and 317V including 'the legitimate expectations of the Australian community relating to privacy and cybersecurity.'[42]

32. However, TARs do not appear to be subject to such decision-making criteria, including reasonableness, proportionality, practicability, technical feasibility and legitimate expectations relating to privacy and cyber security. As individuals' expectations of privacy would appear to be of equal relevance where designated providers voluntarily provide assistance, the OAIC recommends that the decision-making criteria that apply to TANs and TCNs, and the matters to be consider when applying those criteria, be extended to TARs.

33. The OAIC understands that the provisions in Schedule 1 do not require the existence of a warrant before a TAR, TAN or TCN is issued. However, the OAIC also recognises that s 317ZH has been inserted to ensure that a TAN or TCN 'cannot be used as an alternative to a warrant or authorisation.'[43] To complement this section, the OAIC recommends that ss 317RA and 317ZAA be amended to include an additional requirement to consider whether such a warrant is already in place for accessing particular content, when assessing whether a TAN or TCN is reasonable and proportionate.

---

[41] Section 254 of the IPA.

[42] Section s 317RA(f) and s 317ZAA(f) in Schedule 1 of the Bill.

[43] See paragraph 265 of the explanatory memorandum.

Annual reporting

34. To further support transparency and provide an ongoing evidence-base for the necessity and effectiveness of these measures, the OAIC recommends broadening the annual reporting requirements in s 317ZS. For example, annual reports issued by the Minister for Home Affairs on the use of telecommunications interception and surveillance devices by Australian agencies under the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* include information and statistics about agencies that have intercepted or accessed telecommunications, or used surveillance devices; the type of warrants applied for, or the type of surveillance devices used; and the number of prosecutions and convictions resulting from the use of intercepted or accessed telecommunications information, or from the use of surveillance. The OAIC recommends that the Bill include these kinds of reporting obligations for TARs, TANs and TCNs.

Sunset clause

35. The OAIC recommends including a sunset clause to provide industry, enforcement and security agencies, and the public with assurance that the Parliament will consider the effectiveness of the scheme and any oversight measures within a definite timeframe. Alternatively, a provision requiring review of the scheme after a designated time period could be considered. Section 187N of the TIA Act may provide a useful model, which requires a review by the Parliamentary Joint Committee on Intelligence and Security of the operation of the data retention scheme in Part 5-1A of the TIA Act between the second and third anniversaries of the end of the implementation phase of that Part of the TIA Act.

36. The OAIC is available to provide further information or assistance to the Committee as required.

Yours sincerely,

Angelene Falk
Australian Information Commissioner
Privacy Commissioner

15 October 2018