Australian Government
Office of the Australian Information Commissioner

Our reference: D2018/009716

Department of Home Affairs

By email: [redacted]

Consultation draft – Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the draft Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the draft Bill) and explanatory document, and appreciates the Department's engagement with this office about this proposal.

Under the *Privacy Act 1988* (Cth) (Privacy Act), a function of the Australian Information Commissioner and Privacy Commissioner (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.[1] The Commissioner also has the function of ensuring that any adverse effects of the proposed enactment on the privacy of individuals are minimised.[2]

The objects of the Privacy Act, for which the OAIC has regulatory oversight, include to 'promote the protection of the privacy of individuals' and to 'implement Australia's international obligations in relation to privacy.'[3] A central principle in the Privacy Act is data security – regulated entities must take reasonable steps to protect the security of personal information[4] and must notify individuals and the OAIC in the event of a serious data breach.[5]

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.[6] For new law enforcement initiatives that may adversely impact privacy, this includes demonstrating the necessity of

---

[1] Privacy Act, s28(2)(a)

[2] Privacy Act, s 28(2)(c)

[3] Section 2A of the Privacy Act

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

[5] 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.

[6] 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. (see https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx)

the proposal through evidence, and ensuring that the scope of proposed measures is as clear 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.

The draft 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.[7] These include new powers in Schedule 1 to issue technical assistance requests (TARs),[8] technical assistance notices (TANs),[9] and technical capability notices (TCNs).[10] 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.[11] 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.

Accordingly, the OAIC recommends that Schedule 1 of the draft Bill:

- define the terms 'systemic weakness' and 'systemic vulnerability' in s 317ZG
- 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
- require, to the extent possible, prior technical analysis of any 'acts or things' before they are listed in a TAR, TAN or TCN to confirm that the 'acts or things' do not have any unintended effects on security systems
- 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 this does not provide the necessary flexibility, 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
- limit the relevant objectives for which a TAR, TAN or TCN is granted to more serious criminal and national security offences

---

[7] Explanatory document, p 7.

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

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

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

[11] Section 317ZG in Schedule 1 of the draft Bill

- require additional oversight of a proposed notice, before a TAR, TAN or TCN is issued
- extend the decision-making criteria of reasonableness, proportionality, practicability and technical feasibility to TARs
- require privacy impacts to be considered when assessing whether a TAN or TCN is reasonable and proportionate under ss 317P and 317V (as well as for a TAR if the previous recommendation is adopted)
- require consideration of whether a warrant is already in place for accessing particular content or metadata, when assessing whether a TAN or TCN is reasonable and proportionate
- broaden the annual statistics reporting requirements in s 317ZS
- 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

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.

While the Privacy Act generally applies to the Australian Federal Police and to designated communications providers (designated providers)[12] 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[13] 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.[14]

The Privacy Act includes 13 legally-binding Australian Privacy Principles (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

---

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

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

[14] 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.

consented or an exception applies.[15] APP 11 requires APP entities to take reasonable steps to protect personal information they hold, from misuse, interference, loss, unauthorised access, modification or disclosure. As noted in the OAIC's *Guide to Securing Personal Information*, encryption is one mechanism that APP entities can use to satisfy their APP 11 requirements.[16] 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 the event of a data breach and therefore avoid the requirement to notify the OAIC or affected individuals.[17]

Scope and application of TARs, TANs and TCNs

The OAIC welcomes the intent of s 317ZG in Schedule 1 of the draft 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.[18] This includes limitations on:

- requiring the implementation or building of a new decryption capability[19]
- requiring one or more actions that would render systemic methods of authentication or encryption less effective.[20]

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.[21]

These limitations provide an important safeguard – given the fundamental reliance on robust security practices to support Australians' day-to-day communications. 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 as clear and

---

[15] 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)).

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

[17] 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

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

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

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

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

transparent as possible, to enable an evaluation of whether these are reasonable, necessary and proportionate in the circumstances.

'Systemic weakness' and 'systemic vulnerability'

The OAIC recommends that the draft Bill define the terms 'systemic weakness' and 'systemic vulnerability' in s 317ZG. While the explanatory document provides some useful guidance about the meaning of these terms,[22] it does not make clear whether these terms only apply to weaknesses that extend to a broad range of products across the market, or to any security weaknesses that could impact individuals who are not connected to an investigation. 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.

In defining these terms, the OAIC recommends that the Department should 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.[23] For example, the definition might extend to a weakening of security systems affecting any individuals that are not involved in a current investigation. The OAIC also suggests consideration be given to including some further practical examples of systemic and non-systemic weaknesses and vulnerabilities to clarify the scope of this safeguard.

The OAIC notes that the limitation in s 317ZG does not extend to a TAR. As noted in the explanatory document, the limitation that s 317ZG imposes on TANs and TCNs 'protects the fundamental security of systems and products', and ensures that 'a notice cannot jeopardise the security of a wide range of electronic services, devices or software by default, making them vulnerable to interference by malicious actors'.[24] 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 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.

---

[22] For example, the explanatory document states that 'the reference to systemic methods of authentication or encryption does not apply to actions that weaken methods of encryption or authentication on a particular device/s. As above, the term systemic refers to actions that impact a broader range of devices and service utilised by third-parties with no connection to an investigation and for whom law enforcement have no underlying lawful authority by which to access their personal data' (p. 47)

[23] 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.

[24] Explanatory document, p. 47.

The OAIC also recommends that Schedule 1 require, to the extent possible, prior technical analysis of any 'acts or things' before they are listed in a TAR, TAN or TCN, including appropriate security testing, to confirm that the 'acts or things' do not have any unintended effects on security systems.[25] Such a measure may provide additional certainty that the proposed notices in Schedule 1 will not result in an unintended weakening of security systems.

Defined 'acts or things' in s 317E

Section 317E includes a non-exhaustive list of 'acts or things' that may be included in a TAR or a TAN.[26] 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.[27] While the OAIC recognises that in some circumstances it is necessary to provide for flexibility through discretionary powers, limitations on transparency can make it difficult to fully assess the privacy impacts of any proposed information handling practices.[28] 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.

The OAIC recommends that s 317E include an exhaustive list of all 'acts or things' (rather than use discretionary powers or rules) for all TARs, TANs and TCNs. If additional types of 'acts or things' need to be added over time, the primary legislation could be amended - necessitating greater Parliamentary oversight. Alternatively, if this does not provide the necessary flexibility, 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, it may be appropriate to include obligations in the primary legislation to ensure that privacy is given appropriate consideration in the making of the rules.

Oversight and accountability

Schedule 1 in the draft 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

---

[25] 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).

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

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

[28] 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).

intrusions and law enforcement and national security objectives. In this regard, the OAIC acknowledges the current safeguards and oversight measures in the draft Bill, including annual reporting requirements,[29] Ministerial oversight for the issuing of TCNs[30] and a requirement that the senior decision-maker be satisfied that requirements in a TAN or TCN are reasonable, proportionate, practicable and technically feasible (including a reference in the explanatory document, to consideration of wider public interests including any impact on privacy, security and innocent third parties).[31] 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.[32]

Recent community debate in relation to the My Health Record system has demonstrated some level of community concern about the extent to which Australian Government agencies should be able to access health data for non-medical, secondary purposes, and in particular, access by third parties for purposes related to law enforcement such as the protection of the public revenue. While these initiatives and their objectives differ significantly, there will similarly need to be an appropriate balance struck between the legitimate objective of enhancing agencies' access to intelligible data for enforcement purposes and potential privacy impacts on individuals who are not associated with an investigation. In striking this balance, the OAIC recommends that the Department carefully consider the types of serious offences that justify intrusions on individuals' privacy in the manner proposed by the scheme. Additional oversight, accountability and transparency mechanisms may also help to ensure ongoing community support for this initiative.

Additional oversight

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'.[33] 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.

The OAIC understands that judicial review of decisions made under Schedule 1 to issue a TAR, TAN or TCN is available, to ensure that decisions are made within the legal limits of the

---

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

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

[31] Section 317P and 317V in Schedule 1 of the draft Bill and p. 10-11 in the explanatory document.

[32] Section 317ZH and p. 48 of the explanatory document.

[33] Section 254 of the IPA.

relevant powers.[34] However, the OAIC recommends including in Schedule 1 an oversight regime similar to the UK model, to provide for an additional evaluation, as to whether each notice is necessary and proportionate before it is issued.

Requirement to consider impacts on privacy

As noted above, sections 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 explanatory document identifies privacy as an example of a 'wider public interest' to which the decision-maker must have regard when assessing reasonableness and proportionality.[35]

The OAIC notes that TARs do not appear to be subject to the same decision-making criteria, including reasonableness, proportionality, practicability and technical feasibility, as those found in sections 317P and 317V for TANs and TCNs. This also means that the decision-maker is not required to consider 'wider public interests' such as privacy before issuing a TAR. As individuals' expectations of privacy would appear to be of equal relevance where designated providers voluntarily provide assistance, the OAIC recommends that the Department extend the decision-making criteria that apply to TANs and TCNs to TARs.

Also, to provide greater certainty that privacy must be considered in relation to TARs, TANs and TCNs, the OAIC recommends that the draft Bill require consideration of the privacy impacts of a notice before it is issued, including any impacts the notice may have on whether personal information will be protected from misuse, interference, loss, and from unauthorised disclosure, modification or disclosure. Section 180F of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) may provide a useful model of a legislative requirement to consider privacy. Section 180F, which relates to decisions by an authorised officer about the disclosure of telecommunications data to law enforcement agencies, requires the authorised officer to be satisfied on reasonable grounds that any interference with the privacy of any person that may result from a disclosure or use of information or documents is justifiable and proportionate.[36]

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 the intended limitation contained in s 317ZH, which requires that a warrant be in place before accessing private communications or data. To complement this limitation, the OAIC recommends that a decision-maker be required to consider whether such a warrant is already in place for

---

[34] 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 page 11 of the explanatory document.

[35] Pp. 34 and 38 of the explanatory document.

[36] The justifiability and proportionality is to be assessed with regard to the matters outlined in ss 180F(aa)-(b), and includes the gravity of any conduct in relation to which the authorisation is sought, the likely relevance and usefulness of the information or documents, and the reason why the disclosure or use is proposed to be authorised.

accessing particular content or metadata when assessing whether a TAN or TCN is reasonable and proportionate.

Annual reporting

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 also suggests that the annual reporting requirements in s 317ZS be expanded, so that the Minister must also report annually on the number of TARs issued.

Sunset clause

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, the Department could consider a provision requiring review of the scheme after a designated time period. 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.

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

Yours sincerely,

Angelene Falk
Australian Information Commissioner
Privacy Commissioner

12 September 2018