Australian Government

Office of the Australian Information Commissioner

INSLM Review and Report of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Submission of the Office of the Australian Information Commissioner

oaic.gov.au

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide comments to the Independent National Security Legislation Monitor (INSLM) Review (Review), as referred by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), on the *Telecommunications and Other Legislation Amendment (Assistance and Access Act) 2018* (Act).

2. The *Privacy Act 1988* (Privacy Act) confers on the Australian Information Commissioner and Privacy Commissioner (OAIC) a range of privacy regulatory functions and powers. A function of the OAIC 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 OAIC also has the function of ensuring that any adverse effects of the proposed enactment on the privacy of individuals are minimised.[2] In performing functions, the OAIC must have due regard to the objects of the Privacy Act.

3. The OAIC recognises the challenge facing law enforcement, national security and intelligence agencies combating threats to national security in the digital age. The OAIC recognises there is a need to provide these agencies with greater access to information to address today's complex threats, and to enable timely international cooperation.

4. The powers permitted under the Act have the potential to significantly weaken important privacy rights and protections under the Privacy Act. The encryption technology that can obscure criminal communications and pose a threat to national security is the same technology used by ordinary citizens to exercise their legitimate rights to privacy.

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

6. We have made four submissions on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,* as it then was, and the Act following its enactment. In each submission, we have made recommendations to mitigate privacy risks inherent in the regime of access to encrypted communications established by the Act. The adoption of these recommendations would, in our opinion, help ensure an appropriate level of oversight, accountability and transparency relative to any privacy intrusions that may result from law enforcement and national security objectives.

---

[1] Privacy Act, s 28(2)(a)
[2] Privacy Act, s 28(2)(c)
[3] 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>.

7. In this submission, we provide our comments on the following terms of reference for this review:

   - the proportionality of the Act to national security threats, and
   - the appropriateness of safeguards in the Act for protecting the privacy rights of individuals.

8. The recommendations in this submission should be considered in conjunction with comments we made in the following submissions, to which we refer the INSLM for the purposes of this review:

   - the exposure draft of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Bill) to the Department of Home Affairs[4]
   - the first reading version of the *Telecommunications and Other Legislation Amendment (Assistance and Access Bill) 2018*[5]
   - the PJCIS Inquiry into the Act[6] and
   - the review of the amendments made by the Act.[7]

9. In our most recent submissions to the PJCIS dated 26 February 2019 and 25 July 2019, we made the following recommendations that remain unaddressed by amendments to the Act:

   - further clarifying the terms 'systemic weakness' and 'systemic vulnerability', and their interaction with s 317ZG of the Act
   - introducing independent judicial oversight before a technical assistance notice (TAN) or TCN is issued or varied
   - if our recommendation regarding judicial oversight is not accepted, that decisions to issue a TAN or TCN should be subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1997* (ADJR Act) and
   - making technical assessments mandatory rather than at the request of a provider and extending the mechanism to apply to technical assistance requests (TARs) and TANs, in addition to TCNs.

10. The PJCIS published the report from its review of the Act on 3 April 2019. The recommendations made in the report have not fully addressed our concerns. We have reiterated these concerns in

[4] Submission to the Department of Home Affairs dated 13 September 2018 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

[5] Submission to the PJCIS dated 15 October 2018 https://www.oaic.gov.au/engage-with-us/submissions/inquiry-into-the-telecommunications-and-other-legislation-amendment-assistance-and-access-bill-2018-submission-to-the-parliamentary-joint-committee-on-intelligence-and-security/

[6] Submission to the PJCIS dated 26 February 2019 https://www.oaic.gov.au/engage-with-us/submissions/inquiry-into-the-telecommunications-and-other-legislation-amendment-assistance-and-access-act-2018-submission-to-the-parliamentary-joint-committee-on-intelligence-and-security/

[7] Submission to the PJCIS dated 25 July 2019 https://www.oaic.gov.au/engage-with-us/submissions/review-of-the-amendments-made-by-the-telecommunications-and-other-legislation-amendment-assistance-and-access-act-2018-submission-to-the-pjcis/

our submission dated 25 July 2019 and we wish to raise these recommendations for the consideration of the INSLM.

Proportionate to any threat of terrorism, or national security, or both

Proportionality should be assessed in consideration of international human rights obligations

11. Any assessment of the Act's proportionality to threats of terrorism and national security should be considered in the context of Australia's international obligations to uphold rights to privacy, including:

- Article 17 of the *International Covenant on Civil and Political Rights* (Covenant)[8], and
- the *Organisation for Economic Co-operation and Development Privacy Framework* (2013) (OECD Guidelines).[9]

12. The Covenant was ratified by Australia in 1980, which states in Article 17:

> 1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
> 2. *Everyone has the right to the protection of the law against such interference or attacks.*

13. The Privacy Act gives effect to these obligations and which provides a robust, principles-based framework for privacy protection in Australia. These obligations frame privacy as a right, where interference is permissible only when proportionate to the end sought, necessary in the circumstances, and neither arbitrary nor unlawful.

14. The 13 Australian Privacy Principles (APPs) are the cornerstone of the Privacy Act, and set out governance and accountability obligations[10] around the collection,[11] use and disclosure,[12] security[13] and correction[14] of personal information, and individuals' ability to access personal information held about them by regulated entities.[15] Australia's privacy laws recognise the right

---

[8] International Covenant on Civil and Political Rights, New York, 16 December 1966 https://www.austlii.edu.au/au/other/dfat/treaties/1980/23.html

[9] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[10] APP 1 outlines the requirement for an APP entity to manage personal information in an open and transparent way.

[11] See APPs 3, 4 and 5 which all deal with the collection of personal information.

[12] See APPs 6, 7, 8 and 9 which all deal with the use or disclosure of personal information.

[13] APP 11 requires an APP entity to take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

[14] APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

[15] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request. For more information about the APPs see < https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles>, or for detailed guidance see <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/>

to privacy is not absolute and must be balanced with other competing interests, and appropriate limitations and safeguards must be in place.

15. The United Nations High Commissioner for Human Rights (UNHCR) provides further guidelines for when interferences with privacy are deemed necessary for national security:

> *Governments frequently justify digital communications surveillance programmes on the grounds of national security, including the risks posed by terrorism […] Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.*
>
> *In assessing the necessity of a measure, the Human Rights Committee, in its general comment No. 27, on article 12 of the International Covenant on Civil and Political Rights, stressed that that "the restrictions must not impair the essence of the right […]; the relation between right and restriction, between norm and exception, must not be reversed." The Committee further explained that "it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them."*[16]

16. The onus is on the agency to demonstrate an interference with privacy is both necessary and proportionate to the specific risk being addressed. This must be demonstrated each time such an interference is proposed, that is, in the design and review of this Act, and before the issue or variance of any TAR, TAN or TCN is approved.

Clarifying 'systemic weakness' and 'systemic vulnerability'

17. Section 317ZG of the Act limits a TAR, TAN or TCN from requesting or requiring a provider to implement or build a 'systemic weakness' or 'systemic vulnerability' into a form of electronic protection, or from rectifying such a weakness or vulnerability.[17]

18. The Act defines 'systemic weakness' and 'systemic vulnerability'.[18] However, stakeholder concerns about the practical application of these definitions still remain.[19] Terms such as 'whole class of technology' 'target technologies' and 'connected' are ambiguous such that the effect of the limitation on systemic weaknesses and vulnerabilities, and the potential impacts on individual privacy, is therefore still uncertain.

19. The OAIC acknowledges that these terms are complex and that the Act will apply in a wide range of circumstances. However, given the important protections we understand s 317ZG is intended to provide, and the subsequent risks to the security of personal information if the

[16] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[17] Section 317ZG(1).

[18] Section 317B. See also ss 317ZG(4A)–(5).

[19] Parliamentary Joint Committee on Intelligence and Security, Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, see paragraphs 1.40-1.67

meaning of these terms is not sufficiently clear, we recommend further consideration be given to their definition in the legislation and how they interact with s 317ZG.

Recommendation 1

The OAIC recommends that further consideration be given to the way 'systemic weakness' and 'systemic vulnerability' are defined in the legislation and how these terms interact with s 317ZG.

Appropriate safeguards for protecting the rights of individuals

Assessments are only conducted at the request of a provider and are non-binding

20. The OAIC recognises there are existing oversight mechanisms in the Act providing some degree of judicial oversight.

21. Under the Act, the designated communications provider (provider) is able to request an assessment of a TCN to determine whether it should be issued. If requested, the Attorney-General must appoint two assessors, one with technical knowledge and the other who has previously served as a judge.[20] The Attorney-General must have regard to the report that the assessors produce when deciding whether to proceed to give the TCN,[21] but is not obliged to refrain from issuing a TCN if the assessors determine it should not be given.

22. The provisions in s 317WA(7)(a) require the assessors consider:

- whether the proposed TCN would contravene s 317ZG, concerning systemic weaknesses and systemic vulnerabilities,
- whether the requirements imposed by the proposed TCN are reasonable and proportionate,
- whether compliance with the proposed TCN is practicable,
- whether compliance with the proposed TCN is technically feasible, and
- whether the proposed TCN is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed TCN, and

When weighing up these considerations, the greatest weight must be given to whether the TCN would contravene s 317ZG.[22]

23. The OAIC welcomes these provisions, which go some way to providing an appropriate safeguard, however, notes three persisting concerns:

- these assessments are only conducted if the provider requests a review,

[20] Section 317WA(1)–(5).
[21] Section 317WA(11).
[22] Section 317WA

- the recommendations of the assessment are not binding on the Attorney-General's decision to issue a notice, and
- these assessments still apply only to TCNs, and not to TANs.

Judicial authorisation at the time of issue of TARs, TANs and TCNs

24. Law enforcement activities with an impact on privacy require a deliberate and equal increase in oversight, accountability and transparency. The OAIC notes several other stakeholders have expressed concern that judicial authorisation is not required before issuing a TAR, TAN or TCN, as set out at Appendix A of the PJCIS report.[23]

25. In order to build trust and confidence in the framework, as previously submitted, the OAIC recommends the Act be amended to introduce independent judicial oversight before a TAN or TCN is issued or varied. An application to a judge to issue or vary a TAN or TCN should be accompanied by a mandatory technical assessment.

26. A similar power to issue TCNs is granted under the *Investigatory Powers Act 2016* (IPA) in the UK, where judicial authorisation at the time of issue of a notice is required. The approval process requires what is known as a 'double lock' safeguard, requiring the approval of both the Secretary of State and a Judicial Commissioner before a notice is issued to a provider. The Judicial Commissioner is an independent body with the same level of security clearance as the corresponding law enforcement agencies, and has the ability to adequately assess a notice.

Judicial review under the *Administrative Decisions (Judicial Review) Act 1977*

27. The OAIC notes decisions under this Act are not subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). If the above recommendation regarding judicial authorisation of TANs and TCNs is not adopted, and, contrary to our recommendation the current approval process is retained, we recommend introducing judicial review under the ADJR Act. This would provide judicial review avenues under both the ADJR Act and the original jurisdiction of the High Court or the Federal Court of Australia.[24]

Recommendation 2

The OAIC recommends extending the assessment mechanism to TARs and TANs to enhance its effectiveness as an effective safeguard.

[23] Parliamentary Joint Committee on Intelligence and Security, "Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (3 April 2019) https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Report

[24] By operation of s 39B(1) of the *Administrative Decisions (Judicial Review) Act 1977*

Recommendation 3

The OAIC recommends the Act be amended to require independent judicial authorisation before a TAN or TCN is issued or varied.

Recommendation 4

The OAIC recommends that, if Recommendation 3 is not accepted, decisions to issue a TAN or TCN should be subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act).

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

Angelene Falk

Australian Information Commissioner

Privacy Commissioner