OVIC
Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D19/850

12 July 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Committee Secretary,

Review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

Thank you for the opportunity to provide comment on the review of the amendments made to Commonwealth legislation by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (**the Assistance and Access Act**).

My office, the Office of the Victorian Information Commissioner (**OVIC**), has a unique regulatory focus, with combined oversight over privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

Under the PDP Act, my office is responsible for setting standards for the security and integrity of law enforcement data systems and access to law enforcement and crime statistics data, as well as auditing such use under the Victorian Protective Data Security Framework. Further, I have an express function under the PDP Act to make public statements in relation to any matter affecting personal privacy or the privacy of any class of individual.[1] As such, the amendments made by the Assistance and Access Act are of particular interest to my office.

The Committee is required under s 187N of the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**) to review the amendments made by the Assistance and Access Act. The terms of reference of the review are as follows:

- the threshold, scope and proportionality of powers provided for by the Assistance and Access Act;
- authorisation processes and decision-making criteria;
- the scope of enforcement provisions and the grant of immunities;
- interaction with intelligence agencies' other powers;
- interaction with foreign laws, including the United States' *Clarifying Lawful Overseas Use of Data Act*;
- impact on industry and competitiveness; and
- reporting obligations and oversight measures.

[1] Under s 8C(1)(f).

As my office has made two submissions in relation to the Assistance and Access Act, one in response to the Department of Home Affairs' (**DHA**) consultation on the Bill[2] and the other in response to the Committee's previous inquiry on the Bill,[3] my comments relate to the remaining concerns I have since the passage of the Assistance and Access Act.

The threshold, scope and proportionality of powers provided for by the Assistance and Access Act

1. It was pleasing to see many of the Committee's 17 recommendations from the Advisory Report on the Assistance and Access Bill, published in December 2018, reflected in the Assistance and Access Act as passed.

2. While we understand the issues faced by intelligence and law enforcement bodies in the digital age, such as the increasing rate and sophistication of cyberattacks,[4] my office is concerned with the impact these reforms pose for the security and privacy of communications as a whole. Members of the community using communications services subject to these reforms have a reasonable expectation that their communications will remain secure and private, and purchase access to certain services for precisely these reasons.

3. The effectiveness of many of the controls and oversight mechanisms contemplated under the Assistance and Access Act, requires a collective and contemporary understanding of privacy and security risks. I welcome the amendments to the decision-making criteria for the issuing of technical assistance requests (**TARs**), technical assistance notices (**TANs**) and technical capability notices (**TCNs**) to now include an assessment of the necessity and expectations of the community relating to privacy and cyber-security (in the context of assessing the reasonableness and proportionality of the industry assistance measures). However, I have remaining concerns about the level of subject matter expertise required to fully understand evolving privacy and security risks in these contexts.

Subject matter expertise of appointed experts

4. Security itself is a continuously evolving concept – rather than something that can be determined once and then implemented, it is always changing as the software, hardware and techniques in use are updated. Practices and systems that were considered safe only last year may now be considered unwise. To that end, the assessments made by the appointed technical experts and retired judges under s 317WA (upon the request of the designated communications provider, under s 317WA(1)) in relation to TCNs will be crucial to reducing the likelihood of TCNs introducing a systemic weakness to the detriment of communications as a whole.

5. Technical experts appointed as assessors under s 317WA(4) should demonstrate a full understanding of the interactions of all the components of the security ecosystem, as this will be necessary to understand and assess whether or not a TCN could introduce a systemic weakness. Further, to truly avoid the creation of a systemic weakness, I note that the assessor will need to demonstrate an appreciation of the security risks not only in the context of the single TCN, but cumulatively, considering the interactions of multiple TCNs and emerging cyber threats. Without a mechanism for reviewing these interactions holistically, Australia runs the risk of creating a serious vulnerability that neither government nor industry will be aware of, but which malicious actors may discover.

---

[2] Available on OVIC's website, here: https://ovic.vic.gov.au/wp-content/uploads/2018/09/Submission-on-Assistance-and-Access-Bill-2018-.pdf.

[3] Available on OVIC's website, here: https://ovic.vic.gov.au/wp-content/uploads/2018/10/Submission-to-the-Parliamentary-Joint-Committee-on-Intelligence-and-Security-Assistance-and-Access-Bill-2018.pdf.

[4] Further, the Explanatory Memorandum for the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 also notes the need for law enforcement agencies to "retain the ability to combat crime and national security threats notwithstanding advances in technology" [153].

Administrative decision maker's ability to fully appreciate privacy and security risks

6. I have remaining concerns regarding an administrative decision-maker's ability to fully understand the wider security risks in issuing a TAR, TAN or TCN, when considering the "legitimate expectations of the Australian community relating to privacy and cybersecurity" as part of the assessment of the reasonableness and proportionality of a TAR, TAN or a TCN. As a result, in relation to TCNs, I recommend that consideration of the report prepared by the appointed assessors under s 317WA form part of the binding decision-making criteria that the Attorney-General must take into account when deciding whether or not to issue a TCN. I note that the Attorney-General is currently required under s 317WA(11) to have regard to the assessment report prepared under s 317WA(6), which is a welcome measure. However, as this requirement appears to be a relevant consideration for decision-making, I recommend that s 317V, outlining the express decision making criteria of the Attorney-General, refer to s 317WA(11), to clarify the relevant considerations for the Attorney-General's decision to issue a TCN.

Definition of systemic weakness

7. It is positive to see definitions of 'systemic vulnerability' and 'systemic weakness' inserted under the Act. However, I have remaining concerns that these definitions continue to imply that a selective weakness does not create a systemic weakness, suggesting there is a belief that a selective weakness can be adequately secured, or that its re-use will be prevented. Further, these definitions suggest that there is an underlying assumption that only agencies identified under the Act will be able to utilise the weaknesses created under TCNs, for express law enforcement purposes under the Act. However, there is a well-documented risk that malicious actors may take advantage of any weaknesses created.[5] My office recommends that agencies issuing TANs and TCNs ensure that the supporting governance and security arrangements account for the significant security risks the creation of any weakness poses for communications as a whole.

Absence of merits review under the Act

8. My office has previously raised the absence of judicial review under the *Administrative Decisions (Judicial Review) Act 1977* and merits review under the Assistance and Access Act.[6] In the absence of merits review, the insertion of ss 317JC, 317RA and 317ZAA is welcome, although not sufficient to remove our concern. Considering the absence of merits review, as a further safeguard, decision-makers should have access to detailed guidance, setting out the relevant and irrelevant considerations for the purposes of ss 317JAA, 317P and 317V (read with ss 317JC, 317RA and 317ZAA, respectively). Guidance should clearly explain to a non-technical audience what the privacy and wider security impacts (broader than just cybersecurity) of a TAR, TAN or TCN are, or could be, to provide further context to the requirement to consider the "legitimate expectations of the Australian community relating to privacy and cybersecurity" under these provisions. Guidance may also cover matters such as innocent third-party impacts, interests of the agency, interests of the provider, other means to meet objectives, benefits to the investigation, business impact on the provider and whether the provider is the most appropriate person to assist the agency.

---

[5] As observed by Dr Vanessa Teague and Dr Chris Culnane of Melbourne University, in their submission on the Exposure Draft of the Bill, 'Response to consultation on Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018,' "(a)ny decision about...law enforcement access needs to take into account the likelihood that criminals will use the same access vector." See, page 3.

[6] See, OVIC submission to the Parliamentary Joint Committee for Intelligence and Security, inquiry into Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, [27] – [29]. Available here: https://ovic.vic.gov.au/wp-content/uploads/2018/10/Submission-to-the-Parliamentary-Joint-Committee-on-Intelligence-and-Security-Assistance-and-Access-Bill-2018.pdf.

Authorisation processes and decision-making criteria

9. I have continuing concerns about the ability for TARs, TANs and TCNs to be approved and varied orally under the Act. This ability seems to lend itself to social engineering attacks, for example in providing opportunity for people to impersonate law enforcement officers or administrative decision makers over the phone to access systems. Notwithstanding the limitations on the issuing and variation of notices orally under the Act (in the requirement that there be an imminent risk of serious harm or substantial damage to property) and the illegality of impersonating law enforcement, my view is that those limitations do not offer sufficient protection against malicious actors. As such, I recommend that all notices be issued in writing. My office has previously raised this concern with both with the DHA and the Committee during consultations on the Assistance and Access Bill.

Impact on industry and competitiveness

10. In my view, the Act should be clarified having regard to industry concerns and realities. These reforms impose requirements, with serious penalties for non-compliance, that are difficult to interpret and comply with in practice. DHA submitted that these requirements are made clear through guidance given to agencies in relation to TAR, TANs and TCNs.[7] However, I consdider that legislation, particularly with severe penalty provisions, should be clear on its face, without the need to rely on collateral documents, such as guidance or evidence of parliamentary intent.

11. For example, my office previously raised concerns with the DHA about how the unauthorised disclosure of information provisions under s 317ZF operate. My concerns related to the uncertainty as to whether these provisions had the effect of preventing a designated communications provider from informing the information security community of a vulnerability in practice, if one were to arise. DHA suggests in its current submission to the Committee[8] that amendments to the 'administration exception' under 317ZF(3) would help to clarify this. I support this suggestion as the provision attracts a serious penalty. In such cases relevant principles should be included in legislation – as a single source that cannot be changed without parliamentary scrutiny.

12. Consequently, I recommend the Committee consider the need for other amendments throughout the legislation, to clarify the intended interpretation of provisions where there may be uncertainty about how they operate (or are intended to operate) in practice.

Reporting obligations and oversight measures

13. In the context of the current review of the Assistance and Access Act under s 187N of the TIA Act, my office remains concerned about the potential for scope creep of legislative amendments to the *Telecommunications Act 1997* and the TIA Act without proper oversight of the cumulative impact of such amendments.

14. The amendment to s 187N of the TIA Act to provide for the Committee's ongoing review of the amendments made by the Assistance and Access Act provides an important oversight mechanism into the future. However, the cumulative impact of amendments to telecommunications legislation will be difficult to ascertain, due to the isolated nature of amendments and the level of subject matter expertise, both legislative and technical, required to understand the wider impacts of amendments on the telecommunications ecosystem.

---

[7] See, DHA submission to the Parliamentary Joint Committee for Intelligence and Security, inquiry into the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, [246]. Available here: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018.

[8] Ibid.

15. It would be desirable for the Independent National Security Legislation Monitor specifically to consider the cumulative impacts of any such legislative amendments in his review of the amendments made by the Assistance and Access Act, due 1 March 2020 and in any reviews thereafter.

16. Further, the Minister's discretion to expand the scope of 'listed help' in the context of TCNs by legislative instrument under s 317T(5) continues to raise concerns about the potential for scope creep of this legislation, without appropriate scrutiny. The effectiveness of Parliamentary scrutiny where the Minister exercises his power to expand the scope of listed help under s 317T(5) via legislative instrument will depend on the extent to which the impacts of the proposed expansion are properly understood. It is currently unclear to me how Parliament could develop such an informed view as to understand cumulative impacts in isolation. For this reason, I recommend that any expansion to the scope of 'listed help' in the context of TCNs be done so via legislative amendment to the enabling legislation, rather than subordinate legislative instruments.

I thank you again for the opportunity to comment on the amendments made by the Assistance and Access Act. These reforms represent a dramatic expansion of the powers of law enforcement and security agencies, and the degree to which the Government is able to balance this expansion with the rights of individuals is of great interest to my office.

I have no objection to this letter being published by the Committee without further reference to me. I also propose to publish a copy of this letter on the OVIC website but would be happy to adjust the timing of this to allow the Committee to collate and publish submissions proactively.

[redacted]

Yours sincerely

[redacted]

Sven Bluemmel
Information Commissioner