

A1706573

6 December 2018

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

By email to: TOLAbill@aph.gov.au

Dear Mr Hastie

Telecommunications and Other Legislation (Assistance and Access) Bill 2018

Thank you for the opportunity to appear before the Committee on two occasions regarding the *Telecommunications and Other Legislation (Assistance and Access) Bill 2018*. I trust the information we have provided has been useful to the Committee's inquiry. The comments of this Office, in both our submissions and our oral evidence to the Committee, have largely focused on oversight and some technical issues, noting that the policy issue in relation to providing the new powers to law enforcement agencies is a matter for Parliament.

In the recent *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* the Committee has made the following recommendation as part of Recommendation 5:

The IGIS and the Ombudsman should provide assurances directly to the Committee that the amendments agreed to by the Government address their concerns.

This letter is provided to the Committee in response to that recommendation.

Our Office has been working closely with the Department of Home Affairs to provide input to the amendments to the Bill. To assist the Committee I have enclosed a table that summarises the key comments this Office provided on the draft Bill (including amendments up to version identified as *B18EK171.v77.docx 6/12/2018 9:15 AM*) as well as the action taken to address our comments

I particularly welcome the inclusion of inspection and reporting powers for our Office and provisions that require notification to our Office of the use of the powers in Schedule 1.

While there are some instances noted in the table (marked in orange) where our comments did not result in amendments to the Bill, given the urgency to pass this Bill, we consider we can manage the potential impact by engaging directly with agencies about compliance and adjusting our inspection methodologies.

One further issue with the Bill has been identified by my Office this morning, which relates to section 317ZRB(7) which provides that:

Before tabling the copy of the report [by the Ombudsman], the Home Affairs Minister may delete from the copy information that, if made public, could reasonably be expected to:

- (a) prejudice an investigation or prosecution; or
- (b) compromise any interception agency's operational activities or methodologies.

I note that the current procedures of my Office in finalising reports is to provide agencies with an opportunity to provide advice about whether a report contains any operationally sensitive information that should be removed before publication. For this reason, I consider this subsection unnecessary and am concerned about whether it potentially impacts on the statutory independence of the Commonwealth Ombudsman. Given the current urgency, this will be an issue that we monitor and provide advice on when the Bill is reviewed by the Independent National Security Legislation Monitor (as provided by proposed section 6(2)(1D) of the *Independent National Security Legislation Monitor Act 2010*).

Having regard to the urgency of the Bill and the matters set out in this letter, I am satisfied that the Government amendments adequately address the principle concerns that our Office has raised in relation to the Bill.

Finally, if passed, the Bill will expand this Office's administration, inspection and reporting functions. We have provided costings to the Department of Home Affairs and will continue to engage with the Department on that matter.

Please contact me directly on [REDACTED] if you would like to discuss this letter in further detail.

Yours sincerely

[REDACTED]
[REDACTED]
Jaala Hinchcliffe
Acting Commonwealth Ombudsman

Influencing systemic improvement in public administration

Enclosure – Ombudsman comments

Comment	Provision of original Bill	Action taken	New / updated provision of Bill
Lack of oversight and reporting arrangements for Schedule 1 industry assistance powers [submission and comments of 2 December]	N/A	Bill amended to include: <ul style="list-style-type: none"> - Inspection and reporting provisions under Telecommunications Act - Tabling provisions for Minister under Telecommunications Act - Power to inspect notices made in association with warrant or authorisation under the TIA Act or SD Act. 	<ul style="list-style-type: none"> - Section 317ZRB(1)-(5) of Telecommunications Act [p 39-40] - Section 317ZRB(6)-(7) of Telecommunications Act [p 40] - New section 83(4) of the TIA Act [p 41] and new section 55(2B) of the SD Act [p 45]
Lack of authorisation for information about TAN, TCN and TAR to be disclosed to our Office, and for our staff to disclose that information for the purposes of its functions [submission]	Section 317ZF of Telecommunications Act	Bill amended to include our Office in the list of parties to whom information may be disclosed, and for our staff to be included in the list of parties who may disclose that information.	<ul style="list-style-type: none"> - Disclosures TO Ombudsman: section 317ZF(3)(g) [p 28] - Disclosures BY Ombudsman: section 317ZF(5A)-(5C) of Telecommunications Act [p 28]
<i>Resource implications of expanded role under SD Act</i> [submission]	N/A	Office has provided a funding bid to Home Affairs.	N/A

Comment	Provision of original Bill	Action taken	New / updated provision of Bill
Bill does not require computer access warrants to specify any conditions or restriction imposed by the authorising authority (as applies to other SD warrants) [submission]	Section 27D of SD Act	Bill amended to require inclusion of “any conditions subject to which things may be done under the warrant”.	- Section 27D(1)(b)(xii) [p 44]
Suggest term “by name or otherwise” (as applied to computer access warrant) be more clearly defined to avoid ambiguity (submission) [submission]	Section 27D(1)(b)(ix) of SD Act	No amendment – view provided that this would unreasonably narrow the scope of requests that could be made.	
Suggested the expression ‘earliest time’, used in s 27E(7)(k) (concealments) is undefined and ambiguous. Not clear to us why this provision is necessary given there is a mechanism (s 27F) for seeking extensions [submission]	Section 27E(7)(k)	Following submission: Bill amended to require agencies to notify IGIS/Ombudsman of actions taken outside the 28 days.	Section 49B [p 45]

Comment	Provision of original Bill	Action taken	New / updated provision of Bill
<p>Noted the new notification requirements would provide Ombudsman with visibility of cases where action taken outside 28 days, but advised still not clear to us why this provision is necessary given there is a mechanism (s 27F) for seeking extensions [comments on 2 Dec]</p>		<p>Following comments of 2 Dec: HA advised that, for operational reasons, a second request (extension) may not always be feasible.</p>	
<p>Commented it was unclear how the existing prohibition in s 32(4) of the SD Act on doing acts for which a warrant would be required under the TIA Act intersects with new s 32(2A) which provides that 'an emergency authorisation for access to data held in a computer may authorise anything that a computer access warrant may authorise.' [submission]</p>	<p>Section 32(2A) of SD Act</p>	<p>Bill amended to make it clear an emergency authorisation for access to data in a computer may authorise doing something for which a warrant would be required under the TIA Act.</p>	<p>Section 32(4) amended to include words in bold: "Nothing in this Part authorises the doing of anything for which a warrant would be required under the Telecommunications (Interception and Access) Act 1979 (other than subsection (2A) of the section)" (which relates to emergency authorisations) [p 45]</p>

Comment	Provision of original Bill	Action taken	New / updated provision of Bill
<p>Suggested need to include use, storage and destruction requirements for computer access intercept information (as the information generally aligns with that obtained under a TI warrant, which has these obligations) [submission]</p>	<ul style="list-style-type: none"> - TIA definition of 'restricted record' excludes general computer access intercept information - SD definition of 'protected information' excludes general computer access intercept information 	<p>Addressed in original Bill</p>	<p>Section 5(1)(b) of TIA Act inserts "a general computer access warrant or an ASIO computer access warrant" [p 130 of original Bill]</p> <p>Section 46(1)(a) of SD Act [p 113 of original Bill]</p>
<p>Suggested inclusion of computer access warrants in the compensation provisions of the SD Act [submission]</p>	<ul style="list-style-type: none"> - Section 64 of SD Act 	<p>Bill amended to include computer access warrants</p>	<p>Section 64(2) [p 46]</p>
<p>Suggested limitations applied to TAN and TCNs should also apply to TARs [comments on 2 Dec]</p>	<p>Section 317ZH</p>	<p>In the absence of amendments to the Bill, we asked that clear direction be provided in the Explanatory Memorandum that TARs must not be used to overcome the requirement for a warrant or authorisation. Home Affairs confirmed this would occur.</p>	
<p>Written records for TARs – suggest record keeping provisions may not make it clear the need to consider overarching archiving arrangements that apply [comments on 2 Dec]</p>	<p>Section 317ZH(5); 317M(5)</p>	<p>No change to Bill, but HA advised references to Archives Act and maintaining records to assist with inspections will be included in Explanatory Memorandum</p>	<p>N/A</p>