Submission by the Commonwealth Ombudsman

On the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Exposure Draft

Submission by the Commonwealth Ombudsman

10 September 2018

Introduction

The Commonwealth Ombudsman (the Ombudsman) has an oversight role in relation to a number of covert and intrusive law enforcement powers, including under the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), the *Crimes Act 1914* (the Crimes Act) and the *Surveillance Devices Act 2004* (the SD Act).

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill) proposes to amend the abovementioned Acts. Specifically, the Bill seeks to amend the SD Act to address industry identified capability gaps and strengthen law enforcement agencies' ability to collect previously encrypted information.

Our purpose

The purpose of our Office is to:

- provide assurance that the Australian Government entities and prescribed private sector organisations that the Office oversights act with integrity and treat people fairly, and
- influence enduring systemic improvement in public administration in Australia and the region.

Our role

We seek to achieve our purpose through:

- correcting administrative deficiencies through independent review of complaints about Australian Government administrative action
- fostering good public administration that is accountable, lawful, fair, transparent and responsive
- assisting people to resolve complaints about government administrative action; and
- inspecting the compliance of Commonwealth, State and Territory law enforcement, integrity and regulatory agencies with statutory requirements and assessing the administrative practices of agencies in relation to certain covert, intrusive and coercive powers.

The Ombudsman's role in relation to covert and intrusive powers encompasses oversight functions under the TIA Act, the SD Act and Part IAB of the Crimes Act.

This does not involve assessing the merits of any decisions made by an agency to exercise these powers, rather it is the Ombudsman's role to assess the extent to which agencies have complied with the legislation when exercising these powers.

The Office conducts compliance inspections of law enforcement agencies, which involves engaging with agencies, inspecting relevant records and reviewing agencies' processes and systems to assess compliance with certain statutory requirements.

The Office also provides a written report to the Minister for Home Affairs at six-monthly intervals regarding the results of each inspection conducted under s 55 of the SD Act.

The Bill

Schedule 1 of the Bill amends the *Telecommunications Act 1997* to establish new arrangements for intelligence and interception agencies to seek assistance from communications providers. These new arrangements include the introduction of 'technical assistance requests' and 'technical assistance notices' which may be given by the agency head and 'technical capability notices' which may be given by the Attorney-General on behalf of agencies.

Schedule 2 of the Bill establishes a new type of warrant under the SD Act to be applied for by Commonwealth, State and Territory law enforcement agencies, called a computer access warrant. Schedule 2 also amends the TIA Act to ensure consistency with the proposed changes to the SD Act and the *Australian Security Intelligence Organisation Act 1979.*

Schedule 3 of the Bill amends the Crimes Act to enable criminal law enforcement agencies to collect evidence from electronic devices under a search warrant through 'account based data', which is accessing information associated with an online account.

The Department of Home Affairs has sought submissions from industry members, interest groups and the public on the exposure draft of this Bill.

This submission addresses the:

- need for this Office to be designated an authorised recipient of information under the *Telecommunications Act 1997*, and
- potential consequences flowing from the expansion of the Ombudsman's oversight function under the SD Act.

Amendments to the Telecommunications Act 1997

Schedule 1 of the Bill proposes amendments to the *Telecommunications Act 1997*, which authorise the chief officers of interception agencies to make *technical assistance requests* and give *technical assistance notices* to designated communications providers. The chief officer may also request that the Attorney-General give a designated communications provider a *technical capability notice*. In its current drafting, agencies' use of these powers does not appear to be subject to any external oversight. We recommend consideration is given to whether independent oversight of the use of these powers by agencies should be provided for, similar to our oversight of the metadata regime in the TIA Act. In the event this Office is considered for that role, we would echo the comments made by the Inspector-General of Intelligence and Security (IGIS) in their submission, regarding refinements that could be made to the Bill to improve clarity and accountability for agencies.[1]

For the purposes of this Office's oversight of agencies using covert and intrusive powers, agencies may use technical assistance notices and technical capability notices to *give effect to a warrant or authorisation under a law of the Commonwealth* (see sections 317ZH(4) and (5)). As a result, our officers may inadvertently see these notices and associated records when conducting a compliance inspection.

For this reason, we request the proposed section 317ZF be amended to authorise the disclosure of *technical assistance notice information, technical capability notice information and technical assistance request information* to Ombudsman officials for the purpose of exercising our powers

[1] In particular, with respect to proposed sections 317G, 317HA, 317MA, 317P, 317S, 317TA, 317V, 317ZH and 317ZK.

and performing our functions and duties. In addition, we request inclusion in section 317ZF authority for Ombudsman officials to disclose this information in connection with the exercise of our powers and performance of our functions and duties. This will ensure this Office and the agencies we oversight are afforded the same protection under subsections 317ZF(3) and (5) as the IGIS and the agencies it oversights. We also support the comments included in the IGIS submission about the need for consistency with other secrecy provisions.

Expansion of the Commonwealth Ombudsman's oversight under the SD Act

Section 55(1) of the SD Act provides:

> 55 Inspection of records
>
> (1) The Ombudsman must inspect the records of a law enforcement agency to determine the extent of compliance with this Act by the agency and law enforcement officers of the agency.

Under this provision, this Office will have responsibility for oversighting the use of computer access warrants and emergency authorisations for access to data held in computers, as proposed under Schedule 2 of the Bill.

Under our current oversight of the SD Act, we inspect the records of the 18 Commonwealth, State and Territory law enforcement agencies covered by section 6A of the Act in relation to their use of surveillance devices under the Act. Subject to agencies' use of the surveillance device powers, we conduct an inspection every 12 months to assess the extent of the agency's compliance with the Act. We then make a written report to the Minister for Home Affairs at six monthly intervals on the results of each inspection under section 55 of the SD Act. Under section 61(2) the Minister must table the report in Parliament within 15 sitting days after receiving it. Included in our report is an overview of our compliance assessment of all agencies, a discussion of each agency's progress in addressing any significant findings from previous inspections and details of any significant or systemic issues. We may also report on issues other than instances of non-compliance, such as the adequacies of an agency's policies and procedures to ensure compliance with the Act. The proposed amendments to the SD Act are likely to substantially expand this oversight role.

Given the expansion of our function by the proposed amendments, we would welcome the opportunity to discuss with the Department additional resource requirements for this Office to fulfil our function under section 55.

In implementing this expanded role we will work collaboratively with law enforcement agencies to provide advice on best practice in relation to the use of this new covert and intrusive power, in particular any challenges that agencies may face with the introduction of the new warrant type.

Specifying conditions and restrictions on the warrant

Proposed section 27D stipulates what information a computer access warrant must contain. This section is especially important from a compliance perspective, as the warrant is the source of lawful authority for the agency's use of the power and is the record of the issuing authority's decision.

We note the current drafting of section 27D(1)(b) does not include a requirement that the warrant specify any conditions or restrictions imposed by the issuing authority at the time of issue. This is

not consistent with the current requirements for SD warrants in section 17(1)(b)(xi) of the SD Act, which provides:

> 17 What must a surveillance device warrant contain?
>
> (1) A surveillance device warrant must:
>
> (b) specify:
>
> (xi) any conditions subject to which premises may be entered, or a surveillance device may be used, under the warrant.

It would also appear from the reference to 'conditions and restrictions' in sections 27E(1) and 49(2B)(xi) it is intended that conditions and restrictions are able to be imposed by the issuing authority when issuing a computer access warrant. Accordingly, we recommend that section 27D be amended to include provision for any conditions or restrictions imposed by the issuing authority to be specified in the warrant.

Specifying the identity of a person in the warrant

Proposed section 27D(1)(b)(ix) states that a computer access warrant may specify a person *'by name or otherwise'*. The term 'otherwise' is undefined. This may create difficulty for both law enforcement agencies and authorising officers in determining what is required by this provision. While we understand that there may be a policy reason for the term, we recommend consideration be given to whether the category can be more clearly defined.

Concealment

Proposed section 27E(7) provides broad discretion to an agency to undertake a number of acts for the purposes of concealing its activities under the computer access warrant. It provides:

> (7) If any thing has been done in relation to a computer under:
> (a) a computer access warrant; or
> (b) this subsection;
> then, in addition to the things specified in the warrant, the warrant authorises the doing of any of the following:
> (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;
> (d) entering any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);
> (e) entering any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);
> (f) removing the computer or another thing from any place where it is situated for the purposes of doing the things mentioned in paragraph (c), and returning the computer or other thing to that place;
> (g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:
> (i) using any other computer or a communication in transit to do those things; and
> (ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;
> (h) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing mentioned in this subsection;
> (i) any other thing reasonably incidental to any of the above;
> at the following time:
> (j) at any time while the warrant is in force or within 28 days after it ceases to be in force;

> (k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

We note, in particular, that section 27E(7)(k) allows the 28 days after the warrant ceases to be in force provided for in section 27E(7)(j) to be extended to *'the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c)"*.

We are concerned that the expression 'earliest time' is undefined. This creates ambiguity as to how long after the additional 28 day period ceases an agency can continue to take action under section 27E(7)(k). It unclear why agencies are afforded this additional time when the Bill provides a mechanism under section 27F for agencies to seek extension of a computer access warrant for an additional 90 day period. The use of the formal extension framework ensures greater transparency and contemporaneous oversight by an issuing authority where an agency needs additional time to complete concealment action.

We also note there is no requirement under proposed section 49(2B) to record in the report any actions taken for the purposes of concealment. We recommend, as a matter of good administration, that such a requirement be included.

Emergency authorisations and the prohibition on intercepting communications

Proposed section 32(2A) will be inserted into Part 3 of the SD Act and states:

> (2A) An emergency authorisation for access to data held in a computer may authorise anything that a computer access warrant may authorise.

We note that a computer access warrant may authorise agencies to intercept a communication passing over a telecommunications system (see section 27E(2)(h)).

However, section 32(4) of the SD Act states:

> (4) Nothing in this Part authorises the doing of anything for which a warrant would be required under the *Telecommunications (Interception and Access) Act 1979.*

It is unclear to us how proposed section 32(2A), which permits an emergency authorisation to intercept communications in accordance with section 27E(2)(h), will interact with the prohibition in section 32(4). This should be clarified in the Bill.

Obligations regarding general computer access intercept information

The proposed definition of '*general computer access intercept information'* in section 5(1) of the TIA Act is:

> ***general computer access intercept information*** means information obtained under a general computer access warrant by intercepting a communication passing over a telecommunications system

This definition is picked up by section 6(1) of the SD Act for the purposes of the SD Act.

The definition of *'restricted record'* in the TI Act will be amended so as to exclude general computer access intercept information. Similarly, the definition of *'protected information'* under s 44(1) of the SD Act will be amended to exclude general computer access intercept information.

As a result, the obligations on agencies in relation to use, storage and destruction of restricted records or protected information will not apply to general computer access intercept information. The Explanatory Memorandum for the Bill states that 'where agencies want to gain intercept material for its own purpose, they must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act'. Given the nature of the information covered by the definition of 'general computer access intercept information', which is similar in nature of information covered by TI warrants, we recommend that this information should be covered by the use, storage and destruction requirements that apply to restricted records or protected information even when the agency does not want to use the intercept material for its own purpose.

Compensation for loss or injury

Section 64 of the SD Act provides liability by the Commonwealth to pay compensation to a person for loss or injury resulting from the unlawful use of a surveillance device by a Commonwealth law enforcement agency.

We note the Bill does not propose to amend s 64 to extend this obligation to actions taken under a computer access warrant. As proposed section 27E(6) authorises agencies to use force in executing a computer access warrant, we recommend that section 64 be amended to apply to actions taken under computer access warrants.