



Submission by the
Commonwealth Ombudsman

**Inquiry into the impact of the exercise of
law enforcement and intelligence powers
on the freedom of the press**

Submission by the Commonwealth Ombudsman, Michael Manthorpe PSM

July 2019

Introduction

The Office of the Commonwealth Ombudsman (the Office) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) in response to its inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press.

The purpose of the Office is to:

- provide assurance that the organisations we oversight act with integrity and treat people fairly, and
- influence systemic improvement in public administration in Australia and the region.

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
- providing assurance that Commonwealth, State and Territory law enforcement, integrity and regulatory agencies are complying with statutory requirements and have sound administrative practices in relation to certain covert, intrusive and coercive powers.

Of particular relevance to the Committee's inquiry is the Office's role in independently overseeing the use of certain covert, intrusive and coercive powers by law enforcement agencies under the:

- *Telecommunications (Interception and Access) Act 1979* (TIA Act)
- *Surveillance Devices Act 2004* (SD Act), and
- *Crimes Act 1914* (Crimes Act).

We achieve this role by conducting on-site inspections of agencies' records to assess whether agencies have acted in compliance with legislative requirements. However, we do not assess the merits of an agency's decision to exercise the powers. The Ombudsman must report annually or bi-annually to the responsible Minister (the Minister for Home Affairs) on the outcome of those inspections.

A table summarising the Ombudsman's law enforcement oversight responsibilities is included as an attachment to this submission.

We do not have a statutory inspection role in relation to the use of overt law enforcement powers, such as section 3E of the Crimes Act search warrants. However, under the *Ombudsman Act 1976*, the Office can receive complaints from the public about how Commonwealth law enforcement agencies undertake their administrative functions.

Response to Terms of Reference

To assist the Committee in its inquiry, this submission addresses the following Terms of Reference relevant to the Office's role:

- (b) 'the reasons for which journalists and media organisations could become subject to powers in the performance of the functions of law enforcement or intelligence agencies', and
- (c) 'whether any and if so, what changes could be made to procedures and thresholds for the exercise of those powers in relation to journalists and media organisations to better balance the need for press freedom with the need for law enforcement and intelligence agencies to investigate serious offending and obtain intelligence on security threats'.

Reasons journalists and media organisations could become subject to the exercise of powers

When exercising covert, intrusive and coercive powers, law enforcement agencies must satisfy certain legislative thresholds.¹ For example, in order to intercept telecommunications under Chapter 2 of the TIA Act, an agency must:

- be investigating a 'serious offence' punishable by imprisonment of at least seven years,
- submit an application and affidavit to an external issuing authority (such as an eligible judge or nominated Administrative Appeals Tribunal member), and
- be issued with a warrant by that issuing authority.

Where legislative thresholds are met, an agency can exercise the power including in relation to the investigation of a journalist or media organisation.

The Ombudsman is not a merits review body and cannot assess the merits of an agency's decision to exercise a power or an issuing authority's decision to issue a warrant. However, the Office may consider whether an agency provided a decision-maker with all necessary information in accordance with statutory requirements.

Apart from our inspections regarding the mandatory data retention scheme, our assessment of agencies' compliance with legislative requirements does not specifically scrutinise whether the powers were exercised in relation to the investigation of a journalist or media organisation. This is because the legislation does not place additional thresholds or conditions if the investigation involves a journalist or media organisation. We would also often not be aware if the target of the operation or investigation was a journalist because the application or warrant will not necessarily reference their employment.

A journalist or media organisation could be the subject of covert powers if the requisite legislative thresholds are met; for example, if a law enforcement agency was investigating a journalist or media organisation for allegedly breaching a criminal law imposing an imprisonment penalty of three years or more.

¹ See for example determining applications for: SD Act, ss 16, 24, 27C, 34-35A (surveillance device, retrieval and computer access warrants and emergency authorisations, respectively); Crimes Act, ss 15GI, 15GO and 15GV (controlled operation authorities); TIA Act, ss 46, 46A and 48 (telecommunications interception warrants) and s 116 (stored communications warrants).

In relation to the mandatory data retention scheme, Division 4C of Part 4-1 of the TIA Act imposes specific conditions on agencies where telecommunications data is sought to identify a journalist's source. This includes that the agency must first obtain a 'journalist information warrant'. In determining whether to issue a journalist information warrant, the issuing authority must apply a public interest test that weighs up the public interest in issuing the warrant against the public interest in protecting the confidentiality of the identity of the source, as follows:

Section 180T Issuing a journalist information warrant

(2) The Part 4-1 issuing authority must not issue a journalist information warrant unless the Part 4-1 issuing authority is satisfied that:

(...)

(b) the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source in connection with whom authorisations would be made under the authority of the warrant, having regard to:

- (i) the extent to which the privacy of any person or persons would be likely to be interfered with by the disclosure of information or documents under authorisations that are likely to be made under the authority of the warrant; and
- (ii) the gravity of the matter in relation to which the warrant is sought; and
- (iii) the extent to which that information or those documents would be likely to assist in relation to that matter; and
- (iv) whether reasonable attempts have been made to obtain the information or documents by other means; and
- (v) any submissions made by a Public Interest Advocate under section 180X; and
- (vi) any other matters the Part 4-1 issuing authority considers relevant.

As we do not oversight the warrant issuing process, we cannot comment on how the weighing of these public interest considerations operates in practice. **However, the Committee may wish to consider whether this type of additional public interest test would be a useful addition where different law enforcement powers were being exercised in order to identify a journalist's source.**

Changes to procedures and thresholds for the exercise of powers

Potential limit to the application of journalist information warrant provisions

Under s 180H of the TIA Act, before an agency can internally issue an authorisation for the disclosure of telecommunications data for the purpose of identifying a journalist's source, it must obtain a 'journalist information warrant'. This requirement under the mandatory data retention scheme is intended to balance the public interest in protecting journalists' sources with the need for agencies to access the investigative tools necessary to protect the community.

In October 2017, the Office published a report about the inspection we conducted in response to the Australian Federal Police's (AFP) disclosure that it had accessed a journalist's

telecommunications data without a journalist information warrant.² In January 2019, the Office published a subsequent report on the AFP's progress in addressing the non-compliance.³

As a result of our original inspection of the AFP, we identified the following potential limitation in the application of the journalist information warrant provisions under the mandatory data retention scheme.⁴

Where an agency seeks to access telecommunications data of a person (the source) but that person is neither a journalist nor a journalist's employer, the agency is not required to obtain a journalist information warrant to identify the person as a journalist's source.

This is because s 180H(1), as currently drafted, applies a two-limb test to identify when a warrant is required:

(1) An authorised officer of an enforcement agency must not make an authorisation that would authorise the disclosure of information or documents relating to a particular person if:

a) the authorised officer knows or reasonably believes that particular person to be:

- i) a person who is working in a professional capacity as a journalist; or
- ii) an employer of such a person; and

b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source;

unless a Journalist Information Warrant is in force, in relation to that particular person, under which authorised officers of the agency may make authorisations under that section.

If the first limb of this test is not satisfied – i.e. the person whose telecommunications data the agency is seeking to access is not working in a professional capacity as a journalist and is not the employer of such a person – the agency is not required to obtain a warrant before issuing an authorisation and therefore will not be scrutinised by an external issuing authority or a Public Interest Advocate. This is despite the possibility that agencies have sought access to that telecommunications data for the purposes of confirming whether the person disclosed information to a journalist, and therefore whether they are a journalist's source.

The Committee may wish to consider whether the current drafting of s 180H unintentionally limits the application of journalist information warrant requirements.

² See 'A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the *Telecommunications (Interception and Access) Act 1979* – Access to journalist's telecommunications data without a journalist information warrant' (October 2017) <http://www.ombudsman.gov.au/data/assets/pdf_file/0021/78123/Commonwealth-Ombudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf>.

³ See 'A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the *Telecommunications (Interception and Access) Act 1979* – Compliance with Journalist Information Warrant provisions' (January 2019) http://www.ombudsman.gov.au/data/assets/pdf_file/0034/96748/A-report-on-the-Commonwealth-Ombudsmans-inspection-of-the-Australian-Fe....pdf.

⁴ See above n 3, pgs. 3 and 8.

Attachment A

Summary of Ombudsman’s law enforcement oversight

Power	Legislation	Agencies subject to inspection
Controlled operations authorities	<i>Crimes Act 1914</i> – Part IAB	AFP ACLEI ACIC
Delayed notification search warrants	<i>Crimes Act 1914</i> – Part IAAA	AFP
Control orders	<i>Crimes Act 1914</i> – Part IAAB	AFP
Industry assistance requests and notices	<i>Telecommunications Act 1997</i> – Part 15	All State/Territory police forces, plus: AFP ACIC
Telecommunications interceptions	<i>Telecommunications (Interception and Access) Act 1979</i> – Chapter 2	AFP ACLEI ACIC
Stored communications	<i>Telecommunications (Interception and Access) Act 1979</i> – Chapter 3	All State/Territory police forces, plus: ACIC ACCC ACLEI AFP ASIC Corruption & Crime Commission (WA) Crime & Corruption Commission (QLD) Home Affairs IBAC (Victoria)
Telecommunications data (metadata)	<i>Telecommunications (Interception and Access) Act 1979</i> – Chapter 4	Law Enforcement Conduct Commission NSW Crime Commission ICAC (NSW) ICAC (SA)
Surveillance device warrants	<i>Surveillance Devices Act 2004</i>	All State/Territory police forces, plus: ACIC ACLEI AFP Corruption & Crime Commission (WA) Crime & Corruption Commission (QLD) Law Enforcement Conduct Commission NSW Crime Commission ICAC (NSW)