UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

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

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone AO FAAL

Inspector-General of Intelligence and Security

2 August 2019

Table of Contents

Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this submission to the inquiry by the Parliamentary Joint Committee on Intelligence and Security (the Committee) into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press. Information about the role of the IGIS is at **Attachment A**.

This submission responds to an invitation to provide comment following the commencement of the Committee's statutory review of the Act on 8 July 2019.

The terms of reference for the inquiry are:

> a) The experiences of journalists and media organisations that have, or could become, subject to the powers of law enforcement or intelligence agencies performing their functions, and the impact of the exercise of those powers on journalists' work, including informing the public.
>
> b) The reasons for which journalists and media organisations have, or could become, subject to those powers in the performance of the functions of law enforcement or intelligence agencies.
>
> 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.
>
> d) Without limiting the other matters that the Committee may consider, two issues for specific inquiry are:
>
> a. whether and in what circumstances there could be contested hearings in relation to warrants authorising investigative action in relation to journalists and media organisations.
>
> b. the appropriateness of current thresholds for law enforcement and intelligence agencies to access electronic data on devices used by journalists and media organisations.

This submission focuses on the IGIS role in relation to journalist information warrants available to ASIO under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The submission identifies a small number of potential areas for enhancement of these provisions. This submission also briefly comments on the issues for specific inquiry that are identified in the above terms of reference.

This submission does not comment on the policy underlying existing provisions, including the current thresholds for law enforcement and intelligence agencies to access electronic data on devices used by journalists and media organisations. However, IGIS would be happy to comment on any particular proposals that are being considered by the Committee, particularly with respect to any implications for this office's role of overseeing and reviewing the activities of the intelligence agencies for legality and propriety and for consistency with human rights.

Summary of submission

The Committee may wish to consider the following key points raised in this submission:

- IGIS's role is to oversee and review the activities of the intelligence agencies for legality and propriety and for consistency with human rights. This includes a range of powers available to intelligence agencies that could potentially be applied to journalists and media organisations.
- IGIS conducts regular inspections of ASIO warrants, on a sampling basis. IGIS is also able to consider any complaints received from persons affected by, or otherwise involved in, the exercise of ASIO's powers.
- The thresholds that must be met for ASIO to exercise its powers vary. In most cases, there are no special requirements in relation to journalists or media organisations. Nor is there any requirement to notify IGIS if an investigation is commenced in relation to a journalist or media organisation. Nonetheless, IGIS has not identified any specific propriety concerns in relation to journalists or media organisations arising from its inspections of ASIO warrants or investigation of complaints.
- Chapter 4 of the TIA Act includes special requirements that must be met before ASIO can authorise the disclosure of telecommunications data relating to a journalist, if a purpose of the authorisation is to identify a source.
- Section 185D of the TIA Act requires the Director-General of Security to give a copy of any journalist information warrant to the Inspector-General, as soon as practicable after it is issued. The Director-General must also, as soon as practicable after the expiry of the warrant, give the Inspector-General a copy of any authorisation to disclose telecommunications data that was made under the authority of the warrant.
- To date, IGIS has not identified any failures to comply with the legislative requirements of the journalist information warrants scheme.
- The Committee may wish to consider whether it would be desirable to mandate some public reporting mechanisms in relation to journalist information warrants, in addition to ASIO's classified annual reporting. Agencies are best placed to advise the Committee of how, if at all, annual statistical reporting of warrant numbers may prejudice a particular operation.
- The Committee may wish to consider whether it would be appropriate for ASIO to be required to provide a report to the Attorney-General on each journalist information warrant that is issued, consistent with other types of warrants issued under the ASIO Act and TIA Act.

1. Background

1.1 Powers available to intelligence agencies

IGIS's role is to oversee and review the activities of the intelligence agencies for legality and propriety and for consistency with human rights. This includes a range of powers available to intelligence agencies that could potentially be applied to journalists and media organisations.

Of particular relevance are the special powers available to ASIO under the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) and the TIA Act. Subject to legislative safeguards, these powers enable ASIO to search premises; access computers; use surveillance devices; inspect postal articles; intercept telecommunications; and access stored communications and telecommunications data.

IGIS conducts regular inspections of ASIO warrants, on a sampling basis. IGIS is also able to consider any complaints received from persons affected by, or otherwise involved in, the exercise of ASIO's powers.

The thresholds that must be met for ASIO to exercise its powers vary. In most cases, there are no special requirements in relation to journalists or media organisations. Nor is there any requirement to notify IGIS if an investigation is commenced in relation to a journalist or media organisation. Nonetheless, IGIS has not identified any specific propriety concerns in relation to journalists or media organisations arising from its inspections of ASIO warrants or investigation of complaints.

The legal requirements underlying ASIO's access to telecommunications data under Chapter 4 of the TIA Act differ from other intrusive powers and investigative tools available to ASIO in that they include special requirements with respect to journalists and media organisations. These special requirements include consideration of the public interest when deciding whether to issue a warrant, submissions from a Public Interest Advocate, and a requirement to notify IGIS as soon as practicable. These provisions will be the focus of the remainder of this submission.

1.2 ASIO access to telecommunications data – Chapter 4 of the TIA Act

General prohibition on disclosure of telecommunications data

Although not regulating the acquisition of telecommunications data by agencies, section 276 of the *Telecommunications Act 1997* (the Telecommunications Act) prohibits telecommunications carriers, carriage service providers and contractors from disclosing documents or information related to the contents or substance of a communication, carriage services supplied or the 'affairs or personal particulars' of another person.

There are a number of exceptions to this general prohibition contained in both the Telecommunications Act and the TIA Act, including for disclosure of information that is required or authorised under a warrant, or is otherwise required by or authorised under law.[1]

[1] *Telecommunications Act 1997*, s 280(1).

ASIO access to data under Chapter 4 of the TIA Act

Chapter 4 of TIA Act contains provisions enabling telecommunications data, excluding the contents or substance of a communication, to be disclosed to ASIO and enforcement agencies. This type of telecommunications data is commonly referred to as 'metadata'. Chapter 4 enables ASIO and enforcement agencies to issue an authorisation to a relevant carrier or carriage service provider for specific telecommunications data to be disclosed.

In most cases, a warrant or other form of external approval of the authorisation is not required. For ASIO, section 175 allows the Director-General, or any ASIO employee or ASIO affiliate approved by the Director-General as an 'eligible person', to authorise a carrier or carriage service provider to disclose existing information if satisfied that the disclosure would be in connection with the performance by ASIO of its functions. Section 176 allows the Director-General, or any ASIO employee or ASIO affiliate in a position equivalent to, or higher than, SES Band 2 to issue a 'prospective data authorisation', which additionally allows the disclosure of specified information or documents that come into existence over a defined future period.

When combined with section 313(3) of the Telecommunications Act,[2] authorisations under Chapter 4 of the TIA Act effectively oblige the relevant carrier or carriage service provider to disclose the specified data to ASIO.

Journalist information warrants for identifying sources

Chapter 4 of the TIA Act includes special requirements that must be met before ASIO can authorise the disclosure of telecommunications data relating to a journalist, if a purpose of the authorisation is to identify a source. Sections 175 and 176 *must not* be used by ASIO to authorise the disclosure of information or documents relating to a particular person if:

(a) the eligible person 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 eligible person knows or reasonably believes to be a source;

unless a journalist information warrant is in force in relation to that particular person.[3]

To obtain a journalist information warrant (JIW), the Director-General of Security must apply to the Attorney-General and specify the facts and other grounds on which the Director-General considers it

[2] Section 313(3) of the *Telecommunications Act 1997* requires carriers and carriage service providers to 'give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary' for the purpose of (among other purposes) safeguarding national security.

[3] TIA Act, s 180G.

necessary that the warrant be issued,[4] and must provide further information if requested.[5] Section 180L(2) provides that the Attorney-General must not issue a JIW to ASIO unless he or she is satisfied that:

(a) the Organisation's functions would extend to the making of authorisations under Division 3 in relation to the particular person; and

(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 the performance of the Organisation's functions; 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 Attorney-General considers relevant.

There are also special provisions for JIWs to be issued in an emergency, including by the Director-General in circumstances where none of the relevant Ministers are readily available or contactable.[6]

As noted above, these requirements only apply if ASIO is seeking the disclosure of telecommunications data from a carrier or carriage service provider, rather than seeking to obtain data using other tools or techniques.

1.3 IGIS role

Section 185D of the TIA Act requires the Director-General of Security to give a copy of any JIW to the Inspector-General as soon as practicable after it is issued. The Director-General must also, as soon as practicable after the expiry of the warrant, give the Inspector-General a copy of any authorisation to disclose telecommunications data that was made under the authority of the warrant.

IGIS performs regular inspections of ASIO activities as part of its function to oversee and review the activities of the intelligence agencies for legality and propriety and for consistency with human rights. IGIS is also able to conduct detailed inquiries, for which IGIS has strong investigative powers under

[4] TIA Act, s 180J.

[5] TIA Act, s 180K.

[6] TIA Act, s 180M.

Inspector-General of Intelligence and Security Act 1986, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises.

ASIO advises that it regards the number of JIWs, if any, that have been issued to ASIO as being classified. However, the 2016-2017 IGIS annual report noted:

> In the course of our regular inspections we have observed that ASIO staff are familiar with ASIO internal policies and procedures relating to journalist information warrants. In one case, ASIO mistakenly obtained call charge records for a telephone service belonging to a newspaper's classifieds service. The metadata was collected due to a typographical error and was subsequently deleted. ASIO's response to this mistaken collection of metadata demonstrated ASIO staff's awareness of the legal requirements for obtaining a journalist information warrant.[7]

Since this time, IGIS has not identified any failures to comply with the legislative requirements of the JIW scheme, or any indications that ASIO has sought to obtain telecommunications data related to a journalist's source outside the scope of Chapter 4 of the TIA Act.

IGIS could also consider any complaints received from service providers, employees or members of the public concerning ASIO's access to telecommunications data under Chapter 4 of the TIA Act. No such complaints have been received in the period since the JIW provisions were introduced. It should be noted, however, that as ASIO's exercise of these powers is covert, the subjects of any JIWs issued to ASIO are unlikely to be aware that their telecommunications data has been accessed.

2. Potential enhancements to journalist information warrants

2.1 Reporting requirements

The Committee may wish to consider whether it would be desirable to mandate some public reporting mechanisms in addition to ASIO's classified annual reporting obligations.[8] Agencies are best placed to advise the Committee of how, if at all, annual statistical reporting of warrant numbers may prejudice a particular operation.

Additionally, the Committee may wish to consider whether it would be appropriate to require ASIO to provide a report to the Attorney-General on each JIW that is issued, consistent with other types of warrants issued under the ASIO Act and TIA Act.[9] Reporting requirements could require ASIO to advise whether the data enabled ASIO to identify the journalist's source(s), and whether the information was shared, or will be shared, with other domestic or foreign agencies.

---

[7] IGIS annual report 2016-2017, p. 17.

[8] *Australian Security Intelligence Organisation Act 1979*, section 94(2A)(h)-(i) requires ASIO's annual report to record the number of journalist information warrants and associated authorisations issued during the reporting period. This component of ASIO's annual report is not disclosed publicly.

[9] *Australian Security Intelligence Organisation Act 1979*, section 34; TIA Act s 17.

Reporting on journalist information warrants

The Committee may wish to consider whether it would be desirable to mandate some public reporting mechanisms in relation to journalist information warrants, in addition to ASIO's classified annual reporting.

The Committee may wish to consider whether it would be appropriate for ASIO to be required to provide a report to the Attorney-General on each journalist information warrant that is issued, consistent with other types of warrants issued under the ASIO Act and TIA Act.

3. Specific issues for inquiry

The terms of reference for the inquiry identify two specific issues for inquiry by the Committee:

a. whether and in what circumstances there could be contested hearings in relation to warrants authorising investigative action in relation to journalists and media organisations.

b. the appropriateness of current thresholds for law enforcement and intelligence agencies to access electronic data on devices used by journalists and media organisations.

3.1 Contested hearings in relation to warrants

IGIS regularly inspects ASIO warrants as part of its role of overseeing and reviewing the activities of the intelligence agencies for legality and propriety and for consistency with human rights. IGIS notes that ASIO inquiries and investigations are usually covert in nature. Unlike warrants issued to enforcement agencies, ASIO warrants are issued by the Attorney-General and are not subject to judicial oversight. Any introduction of contested hearings into the ASIO warrant process would represent a significant departure from the existing arrangements, and would require careful consideration.

As outlined above, the JIW provisions under Chapter 4 of the TIA Act require the Attorney-General to be satisfied of a public interest test before issuing a warrant that would enable the retained telecommunications data of a journalist to be disclosed to ASIO. In considering this test, the Attorney-General must have regard to submissions from the Public Interest Advocate.[10] The TIA Act regulations require the Public Interest Advocate to be a former judge who has been 'cleared for security purposes to the same level, and at the same frequency, as that required of an ASIO employee'.[11] Before requesting a JIW, the Director-General of Security must give the Public Interest Advocate a copy of the proposed request, which is required to include the facts and other grounds upon which the Director-General considers it necessary that the warrant be issued.[12] The Public Interest Advocate must endeavour to provide a submission to the Director-General 'within a

[10] TIA Act, s 180L(2).

[11] Telecommunications (Interception and Access) Regulations 2017, cl 11(1).

[12] Telecommunications (Interception and Access) Regulations 2017, cl 11(1). See also TIA Act, s 180J.

reasonable period, but no later than seven days after being given the proposed request or application'.[13]

Once a JIW is issued by the Attorney-General, the Director-General must as soon as practicable give a copy of the warrant to the IGIS.[14] This notification assists IGIS in examining the legality and propriety of ASIO's part in the warrant process.

IGIS notes that the public interest considerations and oversight mechanisms that are a feature of the JIW framework do not apply to the warrant frameworks for other, potentially more intrusive, powers available to ASIO. This includes telecommunications interception and stored communications access warrants issued under Part 2-2 and Part 3-2 of the TIA Act; as well as search warrants, computer access warrants, surveillance device warrants, and postal inspection warrants issued under the ASIO Act. Although these powers are each subject to a ministerial warrant process, the Attorney-General is not obliged to take into account any specific public interest factors equivalent to section 180L of the TIA Act, or to obtain submissions from a Public Interest Advocate. Moreover, there is no requirement to specifically inform IGIS about the issue of such a warrant.

3.2 The appropriateness of current thresholds

This submission does not comment on the policy underlying existing provisions, including the current thresholds for law enforcement and intelligence agencies to access electronic data on devices used by journalists and media organisations. However, IGIS would be happy to comment on any specific proposals that are being considered by the Committee, particularly with respect to any implications for this office's role of overseeing and reviewing the activities of the intelligence agencies for legality and propriety and for consistency with human rights.

With respect to the existing JIW provisions, IGIS notes that a JIW is only required in circumstances where a purpose of making the authorisation is to identify another person whom the eligible person knows or reasonably believes to be a source. A JIW therefore may not be required if the purpose of accessing the telecommunications data relates exclusively to the activities of the journalist, or if the same information is obtained from a different source or using a different method.

[13] Telecommunications (Interception and Access) Regulations 2017, cl 14(1).

[14] TIA Act, s 185D(1)(a).

UNCLASSIFIED

Attachment A: Role of the Inspector-General of Intelligence and Security

The Inspector-General is an independent statutory officer who reviews the activities of the following agencies:

- Australian Security Intelligence Organisation (ASIO);
- Australian Secret Intelligence Service (ASIS);
- Australian Signals Directorate (ASD);
- Australian Geospatial-Intelligence Organisation (AGO);
- Defence Intelligence Organisation (DIO); and
- Office of National Intelligence (ONI).

The Office of the IGIS is part of the Attorney-General's portfolio, and was previously located in the Prime Minister's portfolio from its commencement on 1 February 1987 until 10 May 2018. The IGIS is not subject to direction from any Minister on how responsibilities under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) should be carried out.

The *IGIS Act* provides the legal basis for the IGIS to conduct inspections of the intelligence agencies and to conduct inquiries of the Inspector-General's own motion, at the request of a Minister, or in response to complaints. The overarching purpose of the IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. A significant proportion of the resources of the Office are directed towards ongoing inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries, the IGIS has strong investigative powers, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve classified or sensitive information, and the methods by which it is collected. Conducting an inquiry is resource intensive but provides a rigorous way of examining a complaint or systemic matter within an agency. The Inspector-General also receives and investigates complaints and public interest disclosures about the intelligence agencies. These come from members of the public and from current and former agency staff.

In response to the recommendations of the *2017 Independent Intelligence Review*, the Government announced that, subject to the introduction and passage of legislation, the jurisdiction of the IGIS will be extended to include the intelligence functions of the Department of Home Affairs, Australian Federal Police, Australian Criminal Intelligence Commission and Australian Transaction Reports and Analysis Centre. Resources for the IGIS have been increased to allow the office to sustain a full time equivalent staff of 55 (by 2019-20).