PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY REVIEW OF THE MANDATORY DATA RETENTION REGIME

4 JULY 2019

Australia's Right to Know coalition of media organisations welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security review of the mandatory data retention regime of the *Telecommunications (Interception and Access) Act)* 1979 (the TIA Act).

The mandatory data retention regime is a legislative framework which requires carriers, carriage service providers and internet service providers to retain a defined set of telecommunications data for two years, ensuring that such data remains available for law enforcement and national security investigations. Under this framework, approved law enforcement agencies are able to access this data without a warrant.

Concerns expressed in relation to freedom of the press and access to journalists' metadata during the introduction of the legislation resulted in the inclusion of a Journalist Information Warrant scheme (JIW Scheme) at Division 4C of the TIA Act. These amendments entail intelligence organisations and law enforcement wanting to access journalists' data to discover their sources would first have to seek a warrant.

THE JOURNALIST INFORMATION WARRANT SCHEME REQUIRES IMMEDIATE AMENDMENT

While the intention of JIW Scheme may have been well-meaning, as it currently stands it does little to meaningfully deliver its stated aims. The JIW Scheme is poorly drafted, cloaked in secrecy and does nothing to address concerns relating to identification of journalists' sources. In our view the JIW Scheme and related legislation relating to access to journalists' records more broadly require fundamental reconsideration and immediate amendments.

The current investigations and associated AFP raids into reporting by News Corp's Annika Smethurst and the ABC have shone a spotlight on the erosion of fundamental press freedoms that is the cumulative effect of multiple pieces of legislation, including this one. It is critical that any law in this area is proportionate to the concerns the law is seeking to address.

In our view, the JIW Scheme and the Mandatory Data Retention regime do not pass this test. It is now incumbent on this Committee and the Government of Australia to take action to ensure that the public's right to know is appropriately balanced with the harms that are sought to be addressed in relation to national security. The Government's objectives must be clearly stated and well defined and where these objectives may impact on press freedom, the measures to address them must be no more than is reasonably necessary to achieve the

overall national interest, which includes the national interest in open and accountable Government and public administration.

ARTK strongly holds that our recommended amendments to the JIW Scheme and related legislation will assist to ensure the Australian public's right to know is actively considered in 'balancing' the actions of law enforcement and intelligence activities. The recommended amendments are vital to the fundamental role of news reporting in Australia's right to know.

LEGISLATIVE AMENDMENTS REQUIRED

Foremost, we recommend that accessing the metadata and/or content of journalists' communications for any reason or purpose associated with undertaking professional journalistic activity should not be the subject of any authorisation for disclosure, including any warrant issued, under the TIA Act. That is, we believe that journalists who are reporting in the public interest should be exempt from the operation of this legislation.

If this is not accepted, then we strongly contend that the JIW Scheme must be overhauled as detailed below:

1. A Journalist Information Warrant (JIW) is required for ALL warrants sought under the TIA Act when the subject of the warrant is a journalist, media organisation or similar; and

2. An application for a JIW must be contestable and authorised only if the public interest in accessing the metadata and/or content of a journalist's communication outweighs the public interest in NOT granting access; and

3. The JIW Scheme must apply consistently to ASIO and enforcement agencies; and

4. Transparency across all elements of the JIW Scheme is required.

DETAILED ANALYSIS OF RECOMMENDED AMENDMENTS ABOVE

Lack of transparency = Lack of 'evidence'

Unfortunately, our submission is mostly devoid of evidence of the way in which the JIW Scheme has operated and the role played by the PIAs, since the commencement of the JIWS in 2015 because of the secrecy provisions which apply to the applications for, and approvals of, JIWs.

However, we are aware that:

- There has been at least one breach of the TIA Act by the AFP where, in the process of an investigation, an AFP member accessed Call Charge Records and telecommunications data pertaining to a journalist without a Journalist Information Warrant being issued, in breach of the TIA Act;[1]

- The AFP has admitted that they had obtained another journalist's metadata, prior to the commencement of the JIW Scheme, at the request of the Department of Immigration in order to determine the journalist's sources of a story published by *Guardian Australia*[2] that revealed that a Customs vessel had entered deeper into Indonesian waters than previously disclosed. Whilst not in breach of any law, the incident assists to indicate the types of matters in which Commonwealth enforcement authorities consider there to be a greater public interest in disclosure than in the

[1] AFP statement; and reporting AFP admits illegally obtaining journalist's phone records; Police illegally obtained journalist's phone records under new metadata retention regime; Scheming police is spin over data raid
[2] See https://www.theguardian.com/world/2014/apr/17/australian-ship-went-far-deeper-into-indonesian-waters-than-disclosed?CMP=share_btn_tw

protection of fundamental freedoms, such as confidential information, privacy and the public's right to know; and

- At least two PIAs have been appointed[3].

Recent investigations

In addition, three recent events of grave concern to the media involve the use of AFP warrants or other investigative powers directly affecting journalists and related to their confidential sources.

i. First, the AFP raid at the home of News Corp journalist Annika Smethurst on 4 June 2019 involved a search of the entire contents of Ms Smethurst's home in order to identify the source of an article written in April 2018 which suggested that the government was considering allowing surveillance of its citizens by the Australian Signals Directorate;

ii. The raid at the premises of the ABC in relation to documents featured in ABC reporting known as "the Afghan files" about aspects of Australia's special forces in Afghanistan occurring during the period 2009-2013, which had been published in 2017; and

iii. The third incident involved the questioning of 2GB and Sky News journalist, Ben Fordham regarding information which he had broadcast on 2GB to the effect that the Department of Home Affairs was investigating the passage of six asylum seeker boats from Sri Lanka to Australia.

OPTION 1 – EXEMPTION FOR PUBLIC INTEREST REPORTING

We are aware of no evidence to suggest that the accessing of journalists' information to identify confidential sources of news reports plays a sufficiently useful role in the performance of the proper functions of Australia's security and other enforcement agencies that it would outweigh the importance of the public interest in protecting the identity of confidential sources to the media. To the contrary, it is clear that the continued existence of legislative power which allows such access is likely to have a serious chilling effect on public interest reporting in Australia, and is extremely vulnerable to circumvention. Sources of important public interest information are unlikely to make any contact with the media if they fear that those communications can be traced. Similarly, journalists are likely to be wary of publishing reports which expose Government decision making and policy information for fear of being the subject of intrusive search powers, including of their metadata records – for any purpose, not just to identify sources – as a result.

On the basis of the limited amount of information available to us, as indicated above, it is difficult to see how the identification of the source of information in those examples could be said to provide sufficient assistance to the protection of genuine security interests as to outweigh the recognised public interest in protecting the confidentiality of sources. In some cases, the information allegedly provided by the source is simply not significant. In others, it is old and possibly out of date.

The media organisations which comprise ARTK have a proven record of consulting with Government and exercising appropriate editorial discretion to ensure that no matter which would truly threaten Australia's national security is published by them.

It is vital that secretive and extensive disclosure powers are not then used, and do not appear to be used, to prevent and punish the publication of stories which are merely embarrassing for our Government.

[3] Former South Australian Supreme Court judge Kevin Duggan and former Queensland Supreme Court judge John Muir: https://www.smh.com.au/politics/federal/malcolm-turnbull-appoints-exjudges-to-defend-journalists-under-data-retention-laws-20160124-gmczxg.html

Alternatively, ARTK submits that only in cases of investigations relating directly to Australia's national security should journalists' metadata be the subject of any application for access, on the strict conditions outlined below.

OPTION 2 – OVERHAUL OF THE JIW SCHEME

As we have expressed above, if an exemption is not accepted, then the JIW Scheme must be overhauled consistent along four subject areas detailed below.

These changes find support in the recommendations of the Senate Legal and Constitutional Affairs Committee Inquiry into *The current investigative processes and powers of the Australian Federal Police in relation to non-criminal matters,*[4] including that the Commonwealth Government introduces laws regarding accessing information or records from media organisations during investigations by the Australian Federal Police.

We detail our changes below.

JIW required for ALL warrants sought under the TIA Act where the subject is a journalist/media organisation

Presently, a JIW is only required in relation to accessing the metadata relating to a particular person if the relevant authorising person "knows or reasonably believes that particular person to be a journalist or an employee of a journalist and the purpose of the authorisation is to identify another person believed to be a source".

Change is required for two reasons:

i. Presently, a JIW is ONLY required for access to a journalist's metadata but not any other information and data accessible by warrants – for example intercepted telecommunications (dealt with in Chapter 2 of the TIA Act) and stored communications (dealt with in Chapter 3 of the TIA Act). This must be rectified; and

ii. A JIW is only required where the purpose is to identify a source. This is far too narrow and requires amendment. As we have put previously, the JIW is focused on the purpose rather than the effect of accessing the data. However, a JIW should be obtained regardless of whether or not the journalists' data is accessed for the purpose of identifying sources.

    Limiting the application of the JIW process to circumstances where the purpose of data access is to identify journalists' sources provides inadequate protection to journalist's sources which are revealed when the data is accessed for any other purpose – and not subject to the JIW process. This makes the JIW scheme vulnerable to circumvention. There is no case to support the use of disclosure of other information held by journalists.

The application for a JIW must be first approved by the Attorney General and the scheme must be applied equally across the types of applicants involved

It is our strong view that any application for a JIW (including a JIW for journalist's information other than metadata which is dealt with above) must not be made without the Attorney General first approving the making of the application. The application should then be contestable as outlined below.

Requiring the Attorney General to adopt a 'gate-keeper' role at this early stage will ensure that the warrant application process is engaged only once the Attorney General has confirmed that a genuine issue of national security has arisen and that a JIW may be justified in the protection of that interest.

---

4 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/AFP_Inquiry/report/~/media/Committees/Senate/committee/legcon_ctte/AFP_Inquiry/report/report.pdf

The JIW Scheme must apply consistently to ASIO and enforcement agencies

Currently, there are differences which apply to ASIO and enforcement agencies as to whom a request to issue a JIW must be made and the tests which apply to those authorising persons for the purpose of determining those applications.

- In the case of ASIO – the Director General of Security requests the Attorney General to issue a JIW (at section 180J). Under s180L, the Attorney General must not issue a JIW unless they are satisfied that AISO's functions would extend to the making of authorisations to disclose the information in relation to the particular person (i.e. the journalist). Those functions allow disclosure where ASIO "is satisfied that the disclosure would be in connection with the performance by [ASIO] of its functions" (at sections 175 and 176).

- In the case of other enforcement agencies (including the AFP) – an application for a JIW must be made to a Part 4-1 issuing authority, such as a Judge. The issuing authority must not issue a JIW unless satisfied that the warrant is reasonably necessary for making authorisations for certain permitted purposes, namely enforcement of the criminal law (at section 178, finding a missing person (at section 178A), enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue (at section 179), investigation of a serious offence (at section 180), or enforcing foreign and international laws (at section 180A and 180B).

We recommend the JIW Scheme be applied consistently and so must require that:

i. Both ASIO and other enforcement agencies must apply first to the Attorney General for initial approval to make the application and then to an independent third party issuing authority for adjudication;
ii. The issuing authority should be a person who is a judge of a court created by the Parliament only. This would require some simple amendments to s6DC of the TIA Act; by deleting subsections (1)(a)(iii), (1)(b) and (2)(b); and
iii. The issuing authority must not issue a JIW unless satisfied, following a contested application as outlined below, that it is reasonably necessary to do so in the protection of Australia's national security interests.

An application for a JIW must be contestable

It is our strong view that any application for a JIW must be contestable.

This should be done by allowing the journalist or media organisation who is the subject of the warrant application to make submissions as to the public interest in NOT accessing the data/information. This would involve the following steps in aggregate:

- The journalist/publisher being notified of the application for a JIW;
- The journalist/publisher being represented at a hearing, presenting the case for the Australian public's right to know including the intrinsic value in confidentiality of journalists' sources and media freedom;
- That hearing being heard by an independent third party issuing authority with experience in weighing evidence, at the level of Supreme Court, Federal Court or High Court Judge; and
- That independent third party issuing authority making a decision whether or not to authorise the issuing of a warrant after having considered the positions put for each party; and
- A warrant can only be authorised if the public interest in accessing the metadata and/or content of a journalist's communication outweighs the public interest in NOT granting access, including, without limitation, the public interest in:
    - The public's right to know
    - The importance of sources including public sector whistle-blowers

- The protection of identities of sources including but not limited to public sector whistle-blowers
- Media freedom

Other

Additionally, some relatively minor amendments would then be required to the regulations to ensure that:

(a) PIAs are independent of government

In order to make clear that the Prime Minister, having appointed the PIA as a person eligible under s 13(1)(a) or having had that person properly appointed by a former Prime Minister, cannot subsequently change the level of security clearance that he or she "considers appropriate" for that PIA, then reg 24(2)(c)(ii), should be changed to read: "ceases to hold a security clearance to *the* level that the Prime Minister *considered* appropriate *when the person was declared to be a Public Interest Advocate".* Otherwise, the Prime Minister could easily terminate PIAs, contrary to the intention evinced by the restricted grounds of misbehaviour, incapacity and insolvency.

(b) PIAs should be appropriately remunerated for their work

Regulation 20(3) should be amended to enable a PIA to negotiate a higher daily rate with the approval of the Office of Legal Services Coordination or the Attorney-General. It should also be amended to enable a PIA to negotiate terms on which he or she may be paid a higher daily rate on a one-off basis to reflect the necessity to perform more than 6 hours' work in a day, particularly in light of the realistic possibility that applications for JIWs may be made urgently. Both these amendments would be consistent with the *Legal Services Directions 2005* (see Appendix D, cll 5 and 9).

(c) The PIA must have all relevant information before them

Regulation 16 should be amended in two respects.

i. First, the provision of further information to a PIA should be mandatory rather than discretionary.

ii. Second it should be the further information itself, and not merely a summary of it, which is provided to the PIA. This deals with the present gap in the regulations whereby there is a requirement that an applicant for a JIW to ensure that a copy of the proposed request or application is given to a PIA (regs 11(1), 12(1), and 12(2)), but this does not extend to "further information" relating to requests or applications which are given to the Attorney General or Part 4-1 issuing authority under ss 180K or 180R of the Act. No reason is identified in reg 16 for *not* providing the PIA with the further information: the discretion is entirely unstructured and subject to no explicit constraints. In our view, there is no good reason why the PIA should not be provided with the further information (it may be noted that the regulations require that PIAs will either hold relevant security clearance, or be appropriately qualified to deal appropriately with sensitive information, so legitimate secrecy cannot be the reason)

In either case, it is important to bear in mind that the whole scheme of Div 4C of Pt 4-1 is that there are *competing* public interests that must be weighed by the independent third party issuing authority – the public interest in issuing a JIW and the public interest in NOT issuing the JIW.

Transparency across all elements of the JIW Scheme is required

Transparency must be introduced into the JIW application process, as indicated above and such that it be legislated that:

- The journalist must be notified of the application for a JIW; and
- The journalist must be able to obtain representation for the hearing; and
- A record of the hearing must be publicly available.

Further, the public interest in transparent operation of Australian law and enforcement requires the introduction of meaningful annual reporting requirements for the JIW Scheme.

This must include – but not be limited to – disaggregated reporting of the number of applications and authorisations of Journalist Information Warrants made by ASIO and enforcement agencies by each type, and summaries of hearings. This must be a legislated reporting requirement. The reporting should be included in the TIA Act annual report. As there is often an extended passage of time after the end of the financial year that the TIA Act annual report as tabled and made public, we also recommend that the Parliamentary Joint Committee on Intelligence and Security receive the report and it be made public in a more timely fashion.