MEAA SUBMISSION TO THE INDEPENDENT NATIONAL SECURITY LEGISLATION MONITOR'S REVIEW OF THE *TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE & ACCESS) ACT 2018* (TOLA ACT)

September 13 2019

Phone Web

PO Box, 723 Strawberry Hills NSW 2012 1300 656 513 MEAA.org

About MEAA

MEAA is the union and professional association for Australia's creative professionals.

The Media section of MEAA includes people working in TV, radio, print and digital. They include journalists, sub-editors, cartoonists, photographers and graphic designers as well as people working in public relations, advertising, book publishing, online community management and website production.

The MEAA *Journalist Code of Ethics*

Members of MEAA Media are bound by MEAA's *Journalist Code of Ethics*.

Clause 3 of the Code is particularly pertinent to this inquiry in that it relates to journalists and their relationship with confidential sources – a privileged relationship that is acknowledged the world over. It is also recognised in the journalist shield laws that exist in the Commonwealth and all but one state/territory jurisdiction.

Clause 3 of the Journalist Code states:

> *"Aim to attribute information to its source. Where a source seeks anonymity, do not agree without first considering the source's motives and any alternative attributable source.* ***Where confidences are accepted, respect them in all circumstances****."* [MEAA emphasis]

The PJCIS inquiry in the Bill

We note that this review has arisen as a result of the first referral to the INSLM by the Parliamentary Joint Committee on Intelligence and Security under s7A of the *INSLM Act*.

Much of this submission echoes MEAA's submission made to the PJCIS inquiry into the relevant legislation when it was at the Bill stage: the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Assistance and Access Bill)*.

MEAA's previous comments on the Bill

On December 2 2018, MEAA issued a public statement (December 2 2018) calling on the government to reconsider the proposed legislation in order to address concerns about the impact on journalists and their sources.

MEAA said the Bill should not be allowed to proceed in its current form.

MEAA chief executive Paul Murphy said: "This Bill would grant access to the communications data of journalists without any proper judicial oversight, and with no consideration of the need to protect public interest reporting.

"Journalists increasingly rely on encrypted communications to protect the identity of confidential sources. Offering this protection is vital. It gives whistleblowers the confidence to come forward with public interest concerns. In the absence of that confidence many important stories will never come to light."

In its statement, MEAA noted that the PJCIS had received nearly 100 submissions to its inquiry – virtually all raised serious concerns about the impact of the legislation. "Instead of listening to the concerns raised by technology experts, lawyers, privacy advocates and many others, the government is instead seeking to ram the legislation through Parliament…" Murphy said.

"Everyone accepts the need to give our law enforcement and intelligence agencies adequate powers to keep us safe. But weakening encryption is a serious and technically complex exercise, one that no other government has done.

"The risk in ramming through complex legislation with undue haste is that it will actually make us less safe and trample on the very democratic freedoms we are seeking to protect. There needs to be much more careful consideration of the risks this legislation poses."

MEAA's submission

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act) enables:

- Computer access warrants - search warrants to be granted to seize and access computers and other electronic devices;
- Assistance Orders applying to device owners;
- Technical assistance requests and notices applying to designated communications providers to permit law enforcement authorities' access to devices; and
- Remote execution of search warrants.

Although MEAA does not doubt the criminal class's use of digital communications, MEAA is gravely concerned that the enacted legislation is neither reasonable nor proportionate.

The Act as it stands carries too few safeguards and exceeds the threats it seeks to manage. It typifies the sledgehammer to crack a walnut approach that is now commonplace in Government attempts to bolster national security and community safety at the expense of press freedom and the public's right to know what our governments do in our name.

MEAA Media's journalist members are especially concerned that warrants and orders may be issued in cases where matters of public interest have been reported through the provision of information by confidential sources and which attract penalties under the *Commonwealth Crimes Act*.

The breach of such a confidence by a journalist offends MEAA's *Journalist Code of Ethics* and endangers coverage of issues deserving public scrutiny.

Together with the new laws that criminalise journalists and journalism, that allow for the surveillance of journalists through the Journalist Information Warrant scheme in the *Telecommunications (Interception and Access) Act 1979*, and the raft of amendments contained 2018 *National Security Amendment (Espionage and Foreign Interference) Act*, law enforcement agencies' powers have been increased to the point where they have a chilling effect on public interest journalism and threaten the public's right to know.

These extreme powers are often packaged as necessary in the name of "national security". However, in their application, these laws attack press freedom, criminalise legitimate journalism and hinder the free-flow of information to the community – the necessary hallmarks of open and transparent government.

The explanatory information around the introduction of these laws has not demonstrated by example how the application of powers used against journalists and their journalism actually preserves national security or the safety of the community.

Instead, we now have a situation where the homes and offices of journalists and their media employers are raided by government agencies. These raids represent an example of how powers granted to government can trample on press freedom and the public's right to know. They provide a cautionary example of that can go wrong.

For example, the recent raids demonstrate that the need for an urgent response to threats to "national security" is clearly nonsense given a year or more has passed since the news stories in question were

published and broadcast. Also, the news stories at the centre of the raids are demonstrably true; they are clearly in the national interest; and they do not pose a threat to national security or safety.

Furthermore, why are journalists being threatened with, and may yet face, criminal charges for simply doing their job: producing legitimate and accurate journalism in the public interest?

MEAA now submits our concerns over key components of the Act.

Computer Warrants
Under the legislation, a law enforcement agency may apply for a warrant to covertly search electronic devices and access content.

The warrants permit the search of electronic devices to determine whether it is relevant and covered by the warrant, which seems to be a process of reverse logic.

MEAA is concerned that the test for enhanced search warrants of "suspecting on reasonable grounds that evidential material is held in a device" will allow fishing expeditions into the communications activity of an ever-escalating number of citizens, including MEAA's members.

Although the Government asserts that a computer access warrant does not authorise the addition, deletion or alteration of data, the explanatory materials also state that such adjustments can be made "where necessary to execute the warrant".

A recent example of overreach is the warrant utilised by Australian Federal Police during its nine-hour raid on the headquarters of the Australian Broadcasting Corporation. The warrant allowed the AFP to "use any other computer or a communication in transit to access the relevant data; and if necessary to achieve that purposes (sic) – to add, copy, delete or alter other data in the computer…". The ability for warrant to allow a government agency to "add, copy, delete or alter" information on a computer system is an outrageous and frightening development in Australia.

Furthermore, the AFP's keywords search terms were so broad they initially captured 9214 emails and documents – an example of a very wide net being cast in that particular fishing expedition.

Assistance Orders
These can be issued by a judicial officer to require a device owner to provide access to the device where it is reasonably suspected that "evidential material" is held on a device. The penalty for refusing to assist authorities will increase to a maximum of five years' imprisonment.

These measures are not confined to what may be considered serious risks of harm to community safety, but to all forms of misconduct.

It is inappropriate to compel members of the community to permit access to personal information without some regard for the severity and nature of an offence.

Technical Assistance Orders
The legislation seeks the introduction of:

- Technical Assistance Requests (TAR),
- Technical Assistance Notices (TAN), and
- Technical Capability Notice (TCN).

These apply to communications providers operating in Australia.

TARs are voluntary and are issued at agency head (or delegate) level. If the request is acted upon by a provider, that provider and their agents are granted civil immunity.

The TAN is a compulsory order requiring a provider to give assistance wherever capable of doing so. TANs are issued by security and law enforcement agency heads or their delegate(s).

TCNs are also compulsory orders that may only be issued by the Attorney-General. The distinction between a TAN and TCN is that the TCN can require a communications provider to build a capability or functionality to provide the assistance sought. A TAN can only seek the application of mechanisms that already exist.

Notices must be for the purpose of enforcing criminal laws, protecting public revenue or safeguarding national security. Each exercise must be reasonable and proportionate.

MEAA is gravely concerned that judicial approval for the issue of notices is not required, although we are advised that the device for which assistance is being sought must be subject of an underlying search warrant.

MEAA strongly opposes the ability of departmental officers and the Attorney-General being able to issue requests and notices, where only the slimmest of evidential tests may be applied.

Additionally, the proposed transparency of the new regime is fundamentally inadequate. Other than the remote prospect of a compliance audit conducted by the Ombudsman, nowhere is it proposed that detailed public scrutiny of requests, notices, orders and warrants will be possible.

Citizens must be contented with reviewing the annual reports of at least 21 law enforcement agencies to determine the number of new law enforcement instruments applied for and issued.

And recent example show that the annual reports may take a year before they are eventually released to the public and the truth discovered. A July 8 2019 news story states: "Documents prepared by the AFP show investigators were granted two special 'journalist information warrants' in the **2017-18 financial year**, and used those warrants to access journalist metadata on 58 separate occasions." [MEAA emphasis]

Another news story dated July 23 2019 again revealed the tardiness of government reporting: "Police have conducted a series of illegal metadata searches, including Western Australian police obtaining invalid warrants targeting journalists and ACT police accessing data 116 times without proper authorisation. The breaches of the *Telecommunications (Interception and Access) Act* are revealed in a Commonwealth Ombudsman report for the period **July 2016 to June 2017**, tabled in parliament by the government on Monday [July 22 2019]." [MEAA emphasis]

Privacy and Protection

Finally, MEAA must register its strongest objections to enabling Commonwealth agencies to disturb – if not destroy – the integrity of encrypted communications systems.

It seems clear to all outside of law enforcement bodies that allowing such trespasses will lead to widespread breaches of personal and professional privacy and of course, lead to journalists being disabled from ensuring that their sources are protected as their Code of Ethics requires them to do "in all circumstances".

MEAA seeks, as a bare minimum, the incorporation of exemptions for persons engaged in journalism and the media industry to ensure that matters of public interest can continue to be reported without fear of government agencies seeking warrants and orders to pursue journalists that shine the light on matters in the public interest and the public's right to know.