20 January 2015

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Secretary,

The media organisations that are parties to this correspondence – AAP, ABC, APN News & Media, ASTRA, Bauer Media, Commercial Radio Australia, Fairfax Media, FreeTV, MEAA, News Corp Australia, SBS, The Newspaper Works and The West Australian – welcome the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security regarding the *Telecommunications (Interception and Access) Bill 2014* (the Bill).

The right to free speech, a free media and access to information are fundamental to Australia's modern democratic society, a society that prides itself on openness, responsibility and accountability.

There are a number of keystones which are fundamental in Australia to ensure journalists are able to do their jobs. These include:

- The ability for journalists to go about their ordinary business and report in the public interest without the real risk of being jailed;
- Protection of confidential sources;
- Protection for whistle-blowers; and
- An appropriate balance of power between the judiciary, the executive, the legislature and the media.

We are concerned that the Bill does not include sufficient checks and balances and as a consequence may erode freedom of communication and freedom of the press. These concerns are set out in more detail below.

LARGE SCALE SURVEILLANCE IMPACTS NEWS GATHERING

During 2014 we made submissions to the Committee regarding the first two tranches of national security bills, being the *National Security Legislation Amendment Bill (No 1) 2014* and the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*. Those submissions outlined, in detail, how the legislation amplified the risks to the fundamental building blocks of journalism by undermining the confidentiality of sources and by providing inadequate protections for whistleblowers, particularly regarding intelligence information.

The Bill currently before the Committee further increases the degree of difficulty that will be encountered by journalists going about their day-to-day jobs, to report in the public interest particularly as it relates to undermining the confidentiality of sources, and the willingness of sources to come forward and share information including non-classified material, which in turn also makes it more difficult to corroborate information and details, which means it takes longer to get the stories that matter.

A recent report by Human Rights Watch (regarding the US), *With Liberty to Monitor All – How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy*[1] (the report) states that:

> *This situation has a direct effect on the public's ability to obtain important information about government activities, and on the ability of the media to serve as a check on government. Many journalists said it is taking them significantly longer to gather information (when they can get it at all), and they are ultimately able to publish fewer stories for public consumption. …[T]hese effects stand out most starkly in the case of reporting on the intelligence community, national security and law enforcement – all areas of legitimate – indeed, extremely important – public concern.*[2]

The report dedicates a section of the report to the impact of surveillance on journalists.[3] It says:

> *'By its nature, large-scale surveillance often implicates the interests of many people who are not suspected of any wrongdoing.'*[4]

The report goes on to say:

> *While most journalists said that their difficulties began a few years ago, particularly with the increase in leak prosecutions, our interviews confirmed that for many journalists large- scale surveillance by the US government contributes substantially to the new challenges they encounter.* ***The government's large-scale collection of metadata and communications makes it significantly more difficult for them to protect themselves and their sources, to confirm details for their stories, and ultimately to inform the public****.*[5] [emphasis added]

Regarding the increasing concerns about how to maintain confidentiality of sources, and the concerns of both journalists and the sources, the report goes on to say:

> *'Journalists expressed diverse views as to when and why reporting conditions began to deteriorate… The most common explanation, however, was a combination of increased surveillance and the Obama Administration's push to minimize unauthorized leaks to the press (both by limiting government employees' contact with journalists, such as through the Insider Threat Program, and by ramping up prosecutions of allegedly unauthorized leaks, as described above). That trend generates fear among both sources and journalists about the consequences of communicating with one another—even about innocuous, unclassified subjects;'*[6]

And;

> *'Yet, beyond the leak investigations and administrative efforts to prevent leaks, many journalists said that the government's increased capacity to engage in surveillance— and the knowledge that it is doing so on an unprecedented scale—has made their concerns about how to protect sources much more acute and real.'*[7]

---

[1] http://www hrw.org/reports/2014/07/28/liberty-monitor-all-0, *With Liberty to Monitor All - How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*, Human Rights Watch in conjunction with the American Civil Liberties Union (2014), p4
[2] Ibid, p4
[3] Ibid p22-48
[4] Ibid, p12
[5] Ibid p23
[6] Ibid p24-25
[7] Ibid p27

The impact of such is that large-scale surveillance makes it difficult for journalists to communicate with sources securely, with each and every call or email leaving a trail. This means that meeting 'in person' may be the most 'secure' way of maintaining a source. However, such meetings also need to be arranged, which means that even 'in person' meetings are likely to create a record of some sort. Furthermore, some sources may not want to have their identities known at all, including to the journalists that they may work with. In such cases, meeting face-to-face is not an option.

The report says:

> *'[M]any journalists said the amount of information provided or confirmed by sources is diminishing. For one, sources are becoming less candid over email and phone.'*[8]

The report also says that sources are less willing to discuss sensitive matters, including where the matter is not 'classified'. It reports one journalist saying:

> *'[There is] much greater reluctance from sources to talk about sensitive stuff…There just isn't a bright line between classified and not.... There's a huge gray area. That's where the reporting takes place. [But s]ources are increasingly unwilling to enter that gray zone.'*[9]

The report also describes the fear and uncertainty that arises in the media due to large-scale surveillance. The report says:

> *'Journalists interviewed for this report described the difficulty of obtaining sources and covering sensitive topics in an atmosphere of uncertainty about the range and effect of the government's power over them. Both surveillance and leak investigations loomed large in this context—especially to the extent that there may be a relationship between the two. More specifically, many journalists see the government's power as menacing because they know little about when various government agencies share among themselves information collected through surveillance, and when they deploy that information in leak investigations.'*[10]

The cumulative impact of these matters is a chilling effect on news gathering through increasing the perceived risks to sources including whistleblowers – in an environment which has also heightened the risk to news gathering by criminalising some reportage and not providing adequate protections for some categories of whistleblowers (details of which are in our previous submissions to the Committee).

Such an impact is supported by the Human Rights Watch report regarding the situation in the US. It states:

> *'What makes government better is our work exposing information,' argued Dana Priest, a Pulitzer Prize-winning national security reporter at the Washington Post. 'It's not just that it's harder for me to do my job, though it is. It also makes the country less safe. Institutions work less well, and it increases the risk of corruption. Secrecy works against all of us.'*[11]

INTERACTION BETWEEN THE THREE NATIONAL SECURITY BILLS

As noted above, the media organisations that are signatories to this submission have also made submissions to the Committee detailing our concerns regarding the two previous national security bills,

[8] Ibid, p41
[9] Ibid, p41
[10] Ibid, p23
[11] Ibid, p45

being the *National Security Legislation Amendment Bill (No 1) 2014* and the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*.

We are of the view that the Bill currently before the Committee exacerbates the detrimental impact those Bills will have on freedom of the media – the undermining of the confidentiality of sources, the lack of protection for whistleblowers, and the risk of journalists being criminalised – all of which, separately and in aggregate, makes it increasingly difficult for news gathering and reporting in the public interest.

LACK OF DEFINED LIST OF AGENCIES ABLE TO ACCESS METADATA

We note, and support, that the Bill aims to limit the range of agencies and bodies that are able to access telecommunications data (metadata collected under the data retention scheme) and stored communications (the content of a communication).

Regarding agencies able to access telecommunications data, this has been limited to 'enforcement agencies', as outlined in the Explanatory Memorandum to the Bill as:

- *'criminal law-enforcement agencies';* and
- *authorities or bodies that have been declared by the Minister as enforcement agencies, where the agencies satisfy certain criteria which operation and investigative practices evince a clear and genuine need to access historical telecommunications data for their investigations*.'[12]

Section 176A contains the definition of 'enforcement agency,' which includes the list of criminal law-enforcement agencies at section 110A(1), and which also provides discretion to the Minister to declare:

- *the authority or body to be an enforcement agency* (section 176A(3)(a)); and
- *persons specified, or of a kind specified, to be officers of an enforcement agency* (section 176A(3)(b)).

We are concerned that the provision of this wide discretion to the Minister, to declare an authority or body to be an 'enforcement agency' – in addition to the stipulation of criminal law-enforcement agencies – somewhat undermines the aim to restrict those able to access telecommunications data. This is particularly so when the elements for consideration in determining such are non-exhaustive, in that section 176A(4)(f) enables the Minister to have regard to *'any other matter that the Minister considers relevant.'*

The aim of the Bill is expressed in the Explanatory Memorandum as being '*to ensure the availability of a specified range of basic telecommunications data for law enforcement and national security purposes.'*[13]

We reiterate that we do not seek to undermine Australia's national security. However, we are concerned that the discretion at section 176A(f), combined with the lack of a requirement that access to telecommunications data (by authorities or bodies other than criminal law-enforcement agencies) must be for the purpose of law enforcement and national security, means that the intention to restrict access to telecommunications data could in fact be accessed for matters of a lesser nature than that purported to be the purpose of the Bill.

This concern is exacerbated, particularly in the context of our concern regarding the impact surveillance laws, including surveillance laws and access to telecommunications data – particularly without a warrant – will have on maintaining confidentiality of journalists' sources. This heightened concern applies in the context that the data sharing relationships between agencies is unclear. In particular, it is unclear what the position is in relation to an agency that is not declared, but that receives telecommunications data via indirect means.

[12] Op. Cit., at [24]
[13] Op. Cit., at [5]

We acknowledge however, that the ability to extend this regime beyond criminal law-enforcement agencies is limited to some extent in that the declaration is a legislative instrument (at section 176A(3)) and therefore subject to scrutiny by the Parliament.

We also acknowledge that the Explanatory Memorandum states: '*While telecommunications data is less privacy intrusive than content, law enforcement and national security agencies can only access data where a case can be made that this information is reasonably necessary to an investigation.*'[14]

Recommendation

- That the Explanatory Memorandum and the Bill be amended to stipulate that the Ministerial declaration scheme available to request access to telecommunications data be based on demonstrated investigative or operational need *for law enforcement and national security purposes only.*

NO WARRANT REQUIRED

Criminal law-enforcement agencies that are able to access stored communications (the content of a communication) will require a warrant to access that content, however, no warrant will be required by the agencies able, or declared to be able, to access telecommunications data.

The *Data Retention Bill – Proposed Data Set*[15] (Proposed Data Set) states that metadata:

> *'Is not the content or substance of a communication and it is not a person's web-browsing history' – that being that metadata is not the 'content' of a communication.'*[16]

For access to the 'content' of a communication, the Proposed data set states that:

> '*Agencies will continue to need to obtain a warrant to access the content of a communication.*'[17]

Therefore, while agencies will require a warrant to access the 'content' of a communication, a warrant will not be required to access the metadata of a communication.

The source of the difference appears to be articulated in the Explanatory Memorandum, which states that *'telecommunications data is less privacy intrusive than content.'*[18] While we make no comment regarding this claim, it is concerning that a range of data points, which when analysed with inter-linkages with other data sources '*is vital to both reactive investigations into serious crime and the development of proactive intelligence on organised criminal activity and matters affecting national security*'[19] – does not require a warrant to ascertain the bona fides of the access.

We acknowledge that the Bill provides the Commonwealth Ombudsman with oversight of the data retention scheme, while the Inspector-General of Intelligence and Security (IGIS) will continue to oversee access to telecommunications data by the Australian Security Intelligence Organisation (ASIO). According to the Explanatory Memorandum the Commonwealth Ombudsman will have the power to inspect the

[14] Op. Cit., at [10]
[15] http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/ProposeddatasetOctober2014.pdf
[16] Op. Cit., p1
[17] Op. Cit., p1
[18] Op. Cit. at [10]
[19] Op. Cit., at [7]

records of enforcement agencies to ensure that agencies are complying with their obligations, including regarding access to telecommunications data, under the *Telecommunications Interception Act*.

However, it appears that without the checks and balances of a warrant, or some other formal authorisation, the records may be lacking an initial point of reference for assessment.

We also acknowledge that there is a requirement for the Ombudsman to report to the Minister, at the end of each financial annual year, regarding inspections. This is dealt with at section 186J of the Bill. However, if there are no inspections or further investigation under section 186B it appears that the report could lack content. Also, section 186J(7) of the Bill restricts that reporting in the following manner:

> *(7) A report under this section must not include information which, if made public, could reasonably be expected to:*
> *(a) endanger a person's safety; or*
> *(b) prejudice an investigation or prosecution; or*
> *(c) compromise any enforcement agency's operational activities or methodologies.*

Such limitations on reporting, including reporting only on the basis of section 186B inspections, does not seem sufficient to inform the public of the functioning of the scheme.

Recommendations

- In the absence of a warrant-like approval process, a properly functioning reporting process to record access to telecommunications data should be established; and

- An annual report be submitted, including statistics regarding the number of times telecommunications data was accessed, by which agencies, etc. The report should also include the results of any inspections and investigations, including compliance data, and any ensuing recommendations for improvement, including for a well-functioning regime.

It should also be noted that our concerns are heightened by the combination of the lack of a definitive list of agencies able to access telecommunications data and the lack of any requirement for a warrant-like approval process to access telecommunications data.

SPECIFIC TYPES OF DATA TO BE RETAINED YET TO BE ESTABLISHED

As outlined in the Explanatory Memorandum of the Bill[20], proposed section 187A of the Bill establishes the *'types of information and documents that service providers may be required to retain,'*[21] including specified categories at 187A(2).

The specific types of data to be retained under the Government's mandatory data retention scheme will be stipulated in regulations that support the Bill. Those regulations are not currently available for consultation. Rather, the Attorney General's Department has published the Proposed Data Set.

While we do not make any comment regarding the substance of the requirements, we note that given the prominence of the issue, and the content of national security, it would be optimal for public policy reasons to have the details of the data to be retained available for consultation at this time.

[20] http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001/upload_pdf/14242b01EM.pdf;fileType=application%2Fpdf
[21] Op. Cit., at [49]

We urge the Parliament to consider these impacts of the proposed amendments before proceeding with the Bill.