

30 January 2017

Communications Security Branch
Attorney-General's Department
3-5 National Circuit
BARTON NSW 2600
By email: communicationssecurity@ag.gov.au

Dear Mr Kelleher and Ms Sheehan,

The parties to this submission – AAP, ABC, APN News & Media, Australian Subscription Television and Radio Association, Bauer Media Group, Commercial Radio Australia, Community Broadcasting Association of Australia, Fairfax Media, Free TV, MEAA, News Corp Australia, NewsMediaWorks, SBS and The West Australian (collectively, the Joint Media Organisations) – appreciate the opportunity to make a submission to the Attorney-General's Department and the Department of Communications regarding the *Consultation Paper – Access to Retained Data in Civil Proceedings*.

In short, we support a continuation of the prohibition on civil litigants being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime.

Further, the prohibition should continue without any exceptions for civil cases to be able to access data stored solely for the purposes of complying with data retention laws.

Undermining freedom of speech

As the Departments are aware, media organisations were actively involved in the processes associated with the enacting bill, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.

As we have expressed in various consultations and for a, there is already a significant undermining of freedom of speech by the access to, and use of, the telecommunications data journalists data to identify sources within the parameters of potential criminal investigations. We cannot countenance this being extended to civil proceedings.

We stated then, and restate now, that 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.

Reasons why the prohibition should be maintained, without exceptions, include:

Lack of justification

The Consultation Paper lacks justification for civil cases to be able to access telecommunications data. On this basis alone exceptions should not be considered.

So-called ‘safe guards’ would be significantly undermined

Media organisations raised concerns during previous consultations about access to telecommunications data within the framework of criminal proceedings particularly regarding accessing journalists’ telecommunications data to identify sources.

Attempts were made to mollify our concerns at the time by referring to the ‘safeguard’ of a significantly reduced number of agencies that were permitted to access telecommunications –from approximately eighty to twenty-one specified criminal law enforcement agencies. Additional safeguards were described as limiting the circumstances in which those law enforcement agencies may lawfully access data; and substantially expanding the powers of the Commonwealth Ombudsman to oversight access to, and use of telecommunications data by those law enforcement agencies.

These ‘safeguards’ – which we continue to have concerns about – would be further exacerbated if access to the data for civil proceedings was considered or included as an exception by regulation.

Lack of check and balance – so exclusions and exceptions to the prohibition should not proceed

Our concerns are heightened as considerations of potential exceptions would not be subject to parliamentary scrutiny, rather only require regulatory amendment. A regulatory power to provide certain classes of civil litigants with access to retained metadata would represent a further erosion of protection of confidential journalist sources and whistle-blowers.

Again, we cannot countenance accessing data that is kept solely for the purposes of national security and crime being available more broadly and the risks this poses to the ability to report in the public interest.

It is important to note here that the Government implemented the journalist information warrant scheme pursuant to section 180X of the *Telecommunications (Interception and Access) Act 1979*. As the Departments are aware, media organisations have a number of significant outstanding concerns regarding both the ability to use journalists’ data to identify sources including whistle-blowers and the journalist information warrant scheme. Against the backdrop of law enforcement requiring a warrant to access data for the purposes of criminal procedures, it is difficult to contemplate the checks and balances for data accessed for civil proceedings. Again, on this basis we cannot support consideration of anything but a prohibition on data access for civil proceedings.

