Data retention plan amended for journalists, but is it enough?

The House of Representatives has finally passed the third tranche of national security legislation, concerning the mandatory retention of all Australians’ data when they use telecommunications services.

In the wake of concerns about how such data retention could impact upon the media, the government and ALP adopted amendments to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

These amendments entail that law enforcement agencies aside from ASIO wanting to access journalists’ data to discover their sources would first have to seek a warrant.

A public interest advocate based on Queensland’s Public Interest Monitor will be appointed to argue against access to journalists’ data, while a judge will decide on whether the disclosure of the data is in the public interest.

While this might seem to be an improvement to protect journalists and their sources, plenty of problems still remain. As we wrote previously, obtaining a warrant to access journalists’ data is unlikely to be difficult for law enforcement agencies. So the requirement to get a warrant cannot be viewed as an adequate safeguard.

In instances where warrants might be considered onerous, members of law enforcement agencies wanting to uncover journalists’ sources may ignore this procedure. Instead, there is nothing to stop them reverse targeting the retained data of others to see if they have been in contact with known journalists.

While intentions to protect the press with a warrant scheme appear well-meaning, the current manifestation of warrant requirements for journalists in Australia’s data retention scheme would actually do little to meaningfully defend press freedoms.

Look to overseas examples

So what is to be done? Inspiration could be taken from the contested warrants process found in the United States.

In the US, journalists are able to testify in a formal court proceeding to argue to a judge why a warrant should or should not be issued to reveal their source.

While this is similar to what the House of Representatives has passed, one important difference remains: that in the US, the journalists themselves can attend and speak in the court hearing.

This means that the media itself can argue why its reporting is in the public interest prior to the sources being revealed, rather than a public interest advocate doing so on its behalf.

The House of Representatives’ amendments can be seen as ill-thought out and premature at this point particularly given the upcoming inquiry by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the impact of the data surveillance regime has on press freedom in Australia.

What is journalism?

In any event, precisely who a journalist is or what constitutes journalism for the purposes of this extra procedure remain highly problematic.

Other jurisdictions such as the US have developed a very expansive definition of journalism or the media based on the publishing of information or opinion.
In Australia, some people – including the independent senator Nick Xenophon – have suggested starting with the definition contained within the Evidence Act 1995. This definition is based on the function of receiving information and publishing news.

However, in the amendments adopted by the House of Representatives, it seems that it is only professional journalists who will benefit from the warrant process. This is a narrower definition of journalism than even the Evidence Act’s.

Furthermore, it does not adequately protect all those receiving information or publishing news, particularly in light of many people beyond those employed by traditional media organisations using social media to perform these tasks in the public interest.

In any event, the Media, Entertainment & Arts Alliance (MEAA) is still unhappy with this additional safeguard for its members. For the MEAA, the fact that even under the new system journalists would not know whether an application has been made to access their retained data, or that this access has been granted, is still extremely concerning.

Furthermore, the MEAA has good cause to be worried about data retention being used to expose confidential sources. The Australian Federal Police has apparently already been trying to access journalists’ data in order to identify these sources.

In an era of tightening restrictions around reporting in the public interest, some respected voices in the area of security-journalism are sounding stern cautionary warnings about conducting journalism that deals with national security and surveillance issues altogether.

**Others concerned about confidentiality**

In addition, there are still no further safeguards proposed for other professionals who have traditionally enjoyed confidentiality around their communications, such as lawyers, medical practitioners and even parliamentarians.

Indeed, Communications Minister Malcolm Turnbull has termed journalists a “special case” when it comes to increased protection of their retained data.

Nevertheless, the Law Institute of Victoria has again called for communications between lawyers and their clients to be exempted from the data retention proposals, and urged a warrant to be necessary for law enforcement to access these communications.

Australian Lawyers for Human Rights have also written to all ALP and cross-bench MPs and Senators, drawing their attention to the fact their own communications – traditionally protected by parliamentary privilege – will not enjoy an exception from mandatory data retention.

Australian politicians may be interested to note that some Green politicians in the UK are currently challenging the suspected interception of their communications – in contravention of parliamentary privilege – by UK government surveillance schemes.

The government’s mandatory data retention plans, even with the extra requirement for a warrant when it comes to journalists, are still hugely problematic. The requirement to obtain a warrant does not really provide a strong safeguard to ensure journalists can do their work in the public interest.

Other groups who also need confidentiality in their communications currently will not receive it. And none of this detracts the fundamental problems that data retention poses for rights and liberties of everyone in Australia, by introducing a mass monitoring scheme of the whole population, regardless of whether they have committed any sort of crime or engaged in any sort of wrongdoing.

Nor has any substantial evidence been provided that this data retention scheme will actually achieve its stated aim of preventing terrorism and reducing crime rates.
The rush to pass a problematic mandatory data retention package has unfortunately trumped meaningful and patient consideration of the undeniable weight of the evidence stacked against it.