What safeguards are in Australia's data retention plans?

March 5 2015, by Adam Molnar And Angela Daly

Is mass data retention the way to go or should authorities be forced to come back with a warrant to find what they want? Flickr/Rosalyn Davis, CC BY-NC-SA

Prime Minister Tony Abbott wants the mandatory data retention laws passed soon despite a number of concerns still being raised about the proposed legislation.

The Parliamentary Joint Committee on Intelligence and Security (PJCIS)

last week released its report and recommendations on the government's Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

Communications Minister Malcolm Turnbull and Attorney General George Brandis this week said they support all 39 recommendations in the bipartisan report.

So let's take a closer – and critical – look at the recommendation and consider the extent to which they mitigate the privacy and civil liberties dangers that data retention schemes pose.

Similar data retention schemes have been condemned and invalidated for their interference with privacy and civil liberties and are currently under challenge in various countries.

The European example

The Court of Justice of the European Union issued a ruling that invalidated the EU's Data Retention Directive (which is the inspiration for the Australian scheme). The lack of safeguards around the use of, and access to, the data was a key reason the court found the law in breach of the fundamental right to privacy.

In Australia, the PJCIS has disregarded testimony concerning the legal invalidation of mandatory data retention schemes on the basis of their threat to human rights. Instead, it hopes to "manage" threats to privacy and free speech through the inclusion of procedural safeguards in the final text of the Bill.

There are several reasons why this is disconcerting.

Few Australians are probably aware that the Bill formalises an already

existing system of unwarranted lawful access under the Telecommunications Interception Act 1979. The PJCIS is operating on the basis that these laws express an appropriate status quo arrangement to pursue subsequent amendments. But the status quo itself is already a significant problem for human rights and privacy.

Society's reliance on digital technology for our everyday needs places unprecedented amounts of highly intimate communications data into the hands of private telecommunication service providers.

Our routine digital communication logs highly sensitive personal details about our lives, so much so that it seems even Malcom Turnbull knows to avoid its capture.

Judicial controls (when properly conducted) that introduce oversight *prior* to access are an important means to ensure that any lawful access requests are necessary, justifiable and proportionate.

Apart from avoiding mass surveillance regimes altogether (which have been proven to be limited as a strategy for preventing terrorism and reducing crime rates), external judicial controls remain one of the more effective safeguards to introduce accountability in a targeted lawful access scheme.

In the absence of judicial oversight that could safeguard improper access and disclosure, the PJCIS has recommended the Commonwealth Ombudsman serve as an enhanced oversight body.

This follows a now common trend in liberal democracies that entails the removal of judicial oversight and the renaming of underfunded "review bodies" as "oversight bodies" to regulate violations during lawful access and anti-terrorism policies.

The media's concerns

Journalists and citizens will feel the impact of this trend in the context of mandatory data retention legislation in Australia.

The media are justifiably worried about the effect such a scheme would have on the confidentiality of sources and press freedoms more generally.

Experience in other countries such as the US and UK has shown that journalists view mass surveillance schemes such as data retention as producing a "chilling effect" on their work.

The PJCIS has, in its report, acknowledged the problems data retention may pose for journalists. It recommended that:

[…] the question of how to deal with the authorisation of a disclosure or use of telecommunications data for the purpose of determining the identity of a journalist's source be the subject of a separate review by this Committee.

But the MEAA was not impressed by this recommendation for not going far enough, and instead wants to see a media exemption from data retention.

Yet in this age of social media and citizen journalism, a precise definition of who or what a journalist is, as a basis to consider adequate exemption privileges, is no easy task.

In an attempt to remedy the threat to freedom of the press, the PJCIS recommends that agencies provide a copy of all lawful access requests that involve journalists' data be supplied to the Commonwealth Ombudsman (or Inspector General of Intelligence and Security (IGS) in

the case of the Australian Security Intelligence Organisation (ASIO)).

But the Ombudsman is bound by a system of laws that already facilitate a hostile environment for journalists and the protection of free speech. In this context, prior judicial oversight to grant access to journalist sources would similarly provide little consolation as an adequate safeguard.

Problematic law

This brings us to our second point. The law itself is problematic. The "safeguarding" mandates of judicial control and the Commonwealth Ombudsman's investigatory powers act as a compliance mechanism in relation to existing laws on the books.

For example, when these safeguarding powers are read against Section 70 of the Crimes Act which makes it a criminal offence for a public servant to share "any fact or document" with a journalist (which is punishable with two years imprisonment), a violation will not likely be found.

The search for a violation will almost always fall under the auspices of a criminal investigation. Similarly, a judge would provide legal authorisation for lawful access to journalist records given reasonable grounds that the request relates to a criminal investigation under Section 70 of the Crimes Act. The current legal environment undermines the potential for adequate safeguarding as proposed by the PJCIS.

Data isn't just useful in court cases though. It is useful as intelligence when operating within a broader information environment. To this end, the committee is operating on the assumption that this information will only be useful in criminal legal proceedings and not as part of a wider strategy that might involve blackmail, discrimination, suppression or

marginalisation (as Bernard-Keane and O'Donnell have noted). In these instances, judicial oversight could potentially protect against spurious requests.

The PJCIS has also not closed the door entirely on the problems mandatory data retention poses to other professions which have traditionally enjoyed confidential relationships with their clients, such as lawyers and medical practitioners.

The Law Institute of Victoria has expressed strong concerns about the government's data retention proposals, and in particular their impact upon legally privileged relationships. Evidence from the US has shown that surveillance is highly problematic for lawyers attempting to communicate confidentially with their clients.

While the PJCIS has called for a prohibition on civil litigants being able to access telecommunications data, it goes on to suggest that appropriate exceptions to this prohibition be made in regulation.

Claims that the Commonwealth Ombudsman works as an effective oversight body in this legal context are misleading. The Ombudsman monitors "compliance" with the scheme, and therefore, could be more adequately understood as a review body that operates after a harm has occurred.

The Ombudsman also depends on knowledge of a breach which can be difficult in the secretive realm of national security. Unless any of the PJCIS safeguards sit in a constructive legal relationship with a bill of rights, increased transparency, or other laws that support press freedoms and privacy, their effectiveness is compromised.

In any event, none of the proposed safeguards address the fundamental problem that data retention poses for rights and liberties. It introduces 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.

The mass nature of the EU's former data retention scheme was one of the reasons the Court of Justice of the European Union invalidated it. Mass surveillance schemes have also been condemned by the United Nations' High Commissioner for Human Rights.

Until the government realises that preventing terrorism and reducing crime rates often depends on matters other than legislating mass indiscriminate surveillance, the notion of a zero-sum trade between enhanced security at the cost of privacy and civil liberties must be challenged.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation