



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

<http://www.privacy.org.au/About/Contacts.html>

18 July 2019

PJCIS Committee

Review of the Mandatory Data Retention Regime

pjcis@aph.gov.au

Uploaded online via www.aph.gov.au

Review of the Mandatory Data Retention regime

This submission from the Australian Privacy Foundation (“APF”) responds to the review of the mandatory data retention regime by the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

Executive summary and recommendation

The mandatory telecommunications data retention regime should be immediately repealed as it is not consistent with human rights and is not ‘strictly necessary’. This conclusion is consistent with independent reviews of mass data retention surveillance schemes in other jurisdictions, and with the reported abandonment of a key program by the NSA.

This recommendation is discussed in detail below.

General comments

The APF put in a detailed submission opposing the legalisation and expansion of the data retention regime during the original consultation in 2014/2015. At that time, the vast majority of non-government organisations and people opposed the introduction of the regime. Based on the submissions to date for this review, there remains a clear delineation on this between people and non-Government organisations, representing those whose data for every call and online interaction is retained and exposed to wide access; and the Government, whose reach into the lives of Australians is consolidated and expanded.

All of the Government submissions to date (with one major exception) either provide data of usage, or discuss in detail claims that the data retention regime is essential for catching criminals. The major exception is the Australian Human Rights Commission that has raised serious issues with human rights breaches.

The rest of the submissions (with one main exception¹) oppose the data retention regime.

This is not a surprising outcome because it is humans that value their human rights. The Government (although it is run by people) does not seem to value the human rights of the people it governs or even its own workers.

The data retention regime is a breach of our human rights. The Australian Human Rights Commission (AHRC) sets these breaches out clearly in its submission to this review. There would be many more breaches if Australia had comprehensive human rights protections like the United Kingdom and every other first world country.² The submission from Australia's Right to Know which opposes data retention where it impinges on the rights to press freedom is yet another example of a complaint about breaches of human rights that many Australians assume we have, but actually do not.

The data retention regime would have gone through a human rights review as part of the process. For some reason, even when there are breaches of human rights, this legislation passed through that review. That review process is not working. It is just a rubber stamp process.

The fundamental issue here is that the Government is coming to treat all of us as suspects. We could all potentially be committing a crime. Instead we should be treated as citizens (which we are), and be able to rely on the traditional protections against government intrusion unless strictly necessary.

It also has to be said that none of this can be justified on preventing terrorism grounds. The vast majority of the huge amount of intrusions into our privacy here do not relate to terrorism. The claims made in Government submissions do not support a finding that mass retention of communications data on every online and phone interaction of every Australian is a proportionate response, given the threats this creates to our rights and freedoms, and to our personal data security.

The data retention regime is a breach of privacy

The data retention regime is a breach of the privacy rights of all Australians. This is because:

1. It indiscriminately collects personal information from and about everyone regardless of whether they are completely innocent of any crime or not.
2. It collects data to be accessed for crimes or infractions people would consider minor and would not cause significant threat to others, for example, illicit drug use or council fines.

¹ The main exception is a set of churches, the Synod of Victoria and Tasmania Uniting Church, which urge the Government to keep the regime to combat online child abuse. It is notable that the Royal Commission into Institutional Child Abuse did not recommend data retention.

² APF, Australian Law Reform Commission and others have repeatedly noted Australians are atypical in lacking a right to address abuse of their personal information in court, and recommended this be remedied by such a right of legal action. There are similar deficiencies for most other human rights and civil liberties in most jurisdictions in Australia.

3. There are almost no limits on access,³ or independent prior scrutiny such as by warrants.
4. There are no enforceable limits on use. It is unknown how the information is used.
5. Despite Government submissions pointing to serious offences, it allows law enforcement to trawl through data indiscriminately on a particular person, which could lead to absurd situations where a person is charged for another low-level crime of no consequence to public safety.
6. It effectively enables tracking and surveillance citizens who have been accused of no crime
7. There is no independently tested evidence on whether it is effective; most of the figures and anecdotes provided in Government submissions record activity, not effectiveness compared to other less intrusive traditional police and intelligence tools, or necessity.
8. The retention of the data represents a data breach risk for everyone, a series of massive “honeypots”. With data breaches it is not “if” but “when”.
9. The data could be obtained by the Government to track, for example, immigrants, visitors or those working for them or with them, with no way to know this has been done.

Overall, the privacy risks are serious and unacceptable.

Human Rights in Australia (including privacy rights)

The Foundation repeatedly writes submissions highlighting the fundamental problem that Australians do not have adequate privacy protections in their own country. The privacy protections for Australians are vastly inferior to those in Europe and the UK. For example, in the UK people have the following privacy protections:

1. UK has adopted and complies with the *General Data Protection Regulation* (GDPR)
2. UK has a *Human Rights Act*
3. UK has an adequately-funded, active privacy regulator

This means that legislation introduced in Australia is built on an inadequate foundation.

It also means that if we had adequate human rights protections in Australia, the data retention regime would have to be repealed or substantially restricted. This conclusion is not speculation as a mandatory data retention framework adopted by the European Union was successfully challenged by Digital Rights Ireland in the European Court of Justice, based on the absence of ‘proportionality’ between the indiscriminate means required and intrusion into communications privacy.⁴

³ As well as the mandatory scheme created by the retention amendment, telecommunications entities may also voluntarily retain and voluntarily disclose metadata under other parts of the TIA Act regimes, with much less oversight.

⁴ European Court of Justice Press Release 8/4/2014, at <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>.

Recommendations

Australians need adequate protections of their human rights including privacy. The key protections needed are:

- Privacy laws that are benchmarked to (or exceed) the protections in the GDPR, the de facto global standard which many Australian data holders are already working to meet
- A *Human Rights Act*
- An adequately funded, active and tough privacy regulator

If these protections were in place the data retention regime would need to be repealed or significantly amended to require court orders for access.

Breaches of human rights in Australia

We support and agree with the submissions by the AHCR on the breaches of Article 17 and 19 of the *International Covenant on Civil and Political Rights* (ICCPR)⁵ by the data retention regime.

Article 17 deals with the right to privacy. As stated above, Australia has completely inadequate privacy laws. Article 17 provides limited protection but at least it provides some protection (if the Australian Government complied with it).

Metadata is very valuable data. It is also, in our view, personal information. It is personal information because, as already comprehensively demonstrated by journalists⁶ and computer scientists, it can very clearly track a person and their actions. Where people go and what they do is personal. Australia should not be a surveillance/police state, and personal information should be kept private unless there is a compelling and court-ordered reason to get this information.

It is also a fundamental breach of privacy to gather up everyone's metadata for the purpose of fighting crime. This is a step away from putting a microchip in everyone and tracking their every move, and a step towards the oppressive surveillance state that appears to be developing in China. We remain convinced that Australia is moving at breakneck speed to a "Big Brother" style surveillance society. It cannot be justified to spy on everyone to get a few people. This is what the data retention regime seeks to enable. It is inconsistent with human rights and the right to privacy.⁷

Article 19 deals with a right to freedom of expression. Freedom of expression is currently a very topical matter in Australia. There is no doubt that Australians are now going to a lot more trouble

⁵ See <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

⁶ For example, 'Surprise, surprise: my online metadata actually reveals where I've been', ARSTechnica (online), 31 March 2014, <https://arstechnica.com/information-technology/2014/03/surprise-surprise-my-online-metadata-actually-reveals-where-ive-been/>.

⁷ When properly scrutinised, it may also not be worth the effort. See the very high cost per Australian conviction revealed by 2015-2016 costings, and the recently-reported decision by the NSA in the US to abandon a key call retention program because the logistical and legal burdens of keeping it outweigh its intelligence benefits, in D Volz and W Strobel, 'NSA Recommends Dropping Phone-Surveillance Program,' *Wall Street Journal* (online), 24 April 2019 <<https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247>>. This development is of course also relevant to the 'Necessary and proportionate' topic below.

to keep away from the intrusive surveillance of the Government. There is a rising use of encryption for all forms of communication (including by former Prime Minister, Malcolm Turnbull) and the use of Virtual Private Networks. Journalists are suddenly on notice that despite the token gesture of the 'Journalist Information Warrant', the emerging Australian data surveillance regime is a threat to their sources, their stories, and their freedom.

Australians who are tech savvy have sent a clear signal about how they feel about surveillance – they hate it.

Worse, it means that freedom of expression has been impacted by the data retention regime. The secrecy of the regime, justified as protection of 'operations and methods', means that no-one can be sure whether they are at risk of suspicionless surveillance, whether it is transient or constant. The awareness of this oppressive possibility is a threat to not only freedom of expression but also freedom of thought, freedom of movement, freedom of association and other protected rights.

Recommendations

All telecommunications metadata must be included in the definition of 'personal information', because it can be and is used to identify and surveill individuals. Section 187LA (2) TIA Act should be expanded to remove potential doubt about factors like geolocation.

Key protections given traditionally to 'the contents of a communication' in the TIA Act and Telecommunications Act should be extended to telecommunications metadata, both that retained under the mandatory scheme and that which can be 'voluntarily' retained or accessed. This is because the intrusiveness and seriousness of the warrantless, suspicionless retention and use of such metadata is potentially more of a threat to privacy and other fundamental rights than a well-controlled, targeted content interception regime.

Failing this, the current data retention regime is in breach of the ICCPR and must be repealed.

Necessary and proportionate

The data retention regime is neither necessary or proportionate. The limited data about levels of activity provided to this review demonstrates that the data retention regime is being used to spy on thousands of Australians. Despite the assertions and the data provided, there is no convincing evidence provided that many of those thousands of Australians committed any crime, or that the data led to a conviction that was needed on serious widespread public safety grounds, or that would not have been possible with the diligent use of less intrusive methods.

As a demonstration of how heavy-handed and disproportionate the use of the regime is, consider the access for illicit drug offences in NSW (as provided by the NSW Crime Commission in Submission 2). Illicit drug offences can include anything from THC to heroin. Most drug use in Australia is recreational, non-violent and causes no harm. Many countries are considering or have decriminalised or legalised certain drug use. There are many Australians calling for the decriminalisation of drugs. In this context, the 2,086 authorisations under s. 178 (2017-2018) is not an acceptable use of the data retention regime. It does not meet community expectations.

There is only one way to ensure that the access of personal information is both necessary and proportionate and that is, the traditional and effective mechanism of independent court oversight. If the data retention regime is not repealed (as strongly recommended in this submission) the minimum change is to ensure that a court order is required to access data. It is not acceptable to simply trawl through people's personal information in the hope of finding information.

This is one example of the excessive 'scope creep' that has come to pass in a system whose fundamental intrusiveness was originally justified on the basis that it was necessary to fight terrorism or the most serious of other crimes. Other submitters have criticised the pressure for access and use from an ever greater range of bodies for an ever wider and in most cases less serious range of offences, infractions or infringements.

Recommendation

In the event that the data retention regime continues (despite the breach of our human rights), the regime should be amended to require a court order to get access to the data.

The court must consider that the alleged crime is either an allegation of homicide or terrorism.

The range of bodies having access to the data, and the range purposes for which they use it, should be subject to regular and substantial reduction. This is to counteract the intrinsic and demonstrated risk of 'scope creep' (which expands access and usage into ever less warranted domains) and the 'honeypot effect' where once one agency has achieved access, others want it.

Any regulations or determinations issued which expand these parameters should be reviewed with a view to repeal to implement a stricter necessity test, and should be identified as disallowable instruments which must go before the Parliament before implementation.

Evidence used for the review should focus on strict necessity; a detailed scrutiny of outcomes and alternatives rather than activity statistics; and the principle of data minimisation rather than data maximization.⁸

The use of the information

There is no public report (and no requirement to report) on how the data collected is used in sufficient detail for proper review of claims of necessity.⁹ There are multiple risks with big data collections:

- Data breaches
- Misuses of the data
- 'Scope creep' into further uses which have further risks not originally understood
- Diversion of resources from other practices which are more effective, or less risky or intrusive

⁸ See the 'Collect it all' motto of the US NSA, which has recently apparently conceded that the burdens do not justify the intelligence benefit in their key call metadata retention program.

⁹ This applies especially to the scope for 'voluntary' collection and 'voluntary' provision of access under the TIA Act outside the mandatory regime which escape even the keeping of records for inspection in that regime; and collection and access done under s 280 of the *Telecommunications Act 1997*, which escape the oversight of the Ombudsman.

None of those risks have been properly mitigated or dealt with in the current data retention regime. Data breaches happen regularly and data can be misused for other purposes. There needs to be external oversight and auditing to ensure the system is working and to minimise those risks.

Recommendation

The data retention regime must have external oversight by an independent body. The body must have the power to audit and track the use of information.

Access to justice

If the data is accessed improperly, misused or there is a security breach then the Government should be liable to everyone affected for those losses. Unfortunately, there is no access to justice available except by going to Court. This means that most people (with the exception of rich people) have no meaningful access to justice. It is unclear whether the Privacy Commissioner has any jurisdiction here (because of the definition of personal information), however, even if they did it is likely they would not make a decision (as they usually decline to make a decision).¹⁰

Recommendation

Access to justice, including rectification and compensation, should be available for all people against the Government if it fails to keep data secure, or permits misuse or unjustified use. The Privacy Commissioner should be given jurisdiction to investigate complaints and award compensation.

Data retention period

The data retention period of 2 years is excessive. It is not necessary or proportionate. The information provided in many of the Government submissions does not demonstrate these tests are satisfied by the initial two-year retention period, let alone the calls for expansion to six years or more.

Recommendation

The data retention regime should be repealed. However, if it is not, the data retention period should be reduced to 6 months.

Deletion of the data

If the data retention regime continues, it needs to be explicit that the data obtained is deleted if it is not being used in an active criminal investigation. Maintaining a metadata database on all Australians is unacceptable. The various regimes covering voluntary and mandatory data retention in the TIA Act and the Telecommunications Act leave potential for much more extensive retention than is apparent from the mandatory scheme's 2 year period, with diminishing transparency, oversight or justification.

¹⁰ Section 41 of the *Privacy Act 1988* (Cth).

Recommendation

All data not being used in an active serious criminal investigation or any criminal investigation must be deleted. The Government should report on this.

If you have any questions please do not hesitate to contact Kat Lane.

Yours sincerely



Kat Lane,
Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au