Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

31 January 2015

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

Dear Secretary,

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014
SUPPLEMENTARY SUBMISSION

The Australian Privacy Foundation (APF) provided a Submission to the Inquiry, and was invited to appear on Friday 30 January.

The APF regrets that its evidence to the Committee was delayed by four hours and that, possibly as a result, the Committee members remaining in the room at the time had no questions to ask.

Based on the proceedings during the day, we anticipated that a number of questions would be asked.

To assist the Committee, we accordingly provide our responses to some of those questions in written form below, and request that you accept them as further evidence.

Thank you for your consideration.

Yours sincerely,

Dr David Lindsay
Vice-Chair, for the Board of the Australian Privacy Foundation
(03) 9905 5547
david.lindsay@monash.edu.au

Australian Privacy Foundation

Answers to Expected Questions

Q1: Are you satisfied with the process that has been undertaken in the development of this proposal?

The APF applies a set of Meta-Principles to the evaluation of proposals that have significant negative implications for privacy. A copy is attached.

When scored against these Principles, the process for developing the Data Retention Bill has serious defects.

In the development of the Bill, the APF is aware of no serious engagement, by the Government or the Attorney-General's Department (AGD), with NGOs, civil liberties or privacy advocates, and especially not on the question of reasonable alternatives to blanket data retention.

The failure to engage in adequate or appropriate consultation with all but apparent supporters of the proposal has resulted in poor legislation with significant defects. These defects include:

- Serious deficiencies in the understanding of the technology underpinning Internet communications, and of the metadata collection practices of carriers and ISPs, which creates problems for a number of provisions in the Bill, including the way in which the data set is dealt with;
- The potentially serious impacts on legal professional privilege, media shield laws and whistleblower protection, which necessarily arise from over broad data retention laws which require complex legislative exceptions that are difficult to draft and to apply in practice;
- Apparent difficulties in fully appreciating fundamental legal concepts such as 'proportionality' and how these are properly applied to proposals for the mass collection and retention of personal data.

The APF considers that these inadequacies should have been addressed at the drafting stage; and that they would have become apparent if there had been proper consultation. Given the evidence presented by carriers, such as Telstra and Optus, that they have no intention of significantly altering current data retention practices, the case for urgent legislation has not been made. We therefore urge the Committee to recommend a longer period for consultation on the proposal, so that due consideration can be given to reasonable alternatives and the flaws in the Bill appropriately addressed.

Q 2: We have been assured that the data retention scheme that this Bill would create merely ensures that existing capabilities of law enforcement agencies keep up with technological change. Is this accurate?

APF's Response:

That assertion is inaccurate, at least in the following ways.

(1) The data retention proposal imposes new requirements.

The telephone call records that have been available to investigators have always been a byproduct of business operations. Data has only been collected where there has been a business need, and has only been retained for as long as there is a business need. The Bill, however, changes this rationale by requiring that records be kept for the purposes of law enforcement and national security even where there is no business need. This alters the fundamental basis on which such data is retained; and will result in the creation of new data, potentially when that data has never been created in the past.

(2) The data retention proposal encompasses far more forms of communication than has been the case in the past.

Communications practices are changing, and will continue to evolve. The APF is concerned that the application of the data set to evolving forms of communication, when combined with a failure to adequately define what is meant by the 'contents or substance of a communication' for the purposes of the proposed s 187A(4)(a) exception, means that the Bill may potentially require the retention of highly personal data relating to:

- Reading and viewing images;
- Watching videos and listening to audio files;
- Private communications within applications, such as communications within computer games; and
- Computer-to-computer communications which, with the emergence of the Internet of Things, will generate vast volumes of data.

All of this is not entirely clear from the Bill; and arises from the failure of the Bill to adequately confine the data set in the legislation, especially when combined with uncertainties in the wording of the statutory exceptions.

(3) The data retention scheme would likely result in vast increases in accesses by law enforcement agencies to data about people's communications.

The evidence of the State law enforcement agencies indicates that retained data has, in many if not most cases, already become a first resort. In the event that this mass retention scheme were passed into law, the potential exists for almost all investigations to routinely commence with access to these vast databases, sometimes simply in order to generate suspicions and suspects. Although it has been suggested that much of the retained data will sit passively in the relevant data repositories, there is nothing in the Bill to require this. Moreover, the rapid development of Big Data analytics raises the prospects of agencies self-certifying access to quite large data sets on the basis that it is 'reasonably necessary for the enforcement of the criminal law' (TIA Act, s 177(1)).

As explained in our submission to the Committee, the APF strongly supports appropriate access of security agencies and law enforcement agencies to metadata where there is a sufficient nexus with investigations. As further explained in our submission, however, the APF supports raising the threshold for access to non-content data, so that such access must relate to investigations of serious criminal offences. Needless to say, we also support appropriate access for the purposes of investigations of serious threats to national security, provided always that there are proper legal checks and balances.

Especially with the potential for function creep inherent in the Bill as currently drafted, as well as the absolutely central role electronic communications play in the everyday lives of Australians, the APF submits that the Bill represents one of the most significant potential intrusions into privacy ever contemplated by an Australian government. As emphasised below, this is especially the case when it has not been established that existing legal safeguards are adequate.

Q3: We've been assured that there are adequate safeguards already in place. Is this accurate?

APF's Response:

This is inaccurate, at least in the following respects:

(1) Retained data is already accessed without proper justification.

Evidence from State law enforcement agencies made abundantly clear that the imposition of a requirement for judicial authority would not merely result in slower processes and a heavy load on judicial officers. They stated that many of their requests would likely be rejected, because they would be unable to establish reasonable grounds for wanting the access to be approved. The APF

submits that access to personal data should always be based on reasonable grounds which are appropriately related to an investigation of serious crimes or threats to national security. For this reason it is important for an appropriate legal threshold to be established for access to metadata and for procedural safeguards to be established as a check on potentially improper access to such data. Self-certification, based on the internal practices of an agency, is simply no substitute for proper independent review. In this respect, we note that procedural safeguards, such as a warrant, for access to metadata are in place in at least 11 jurisdictions in the European Union; and will need to be established in other EU jurisdictions in order to comply with the ruling of the European Court of Justice.

(2) The data retention scheme would result in the creation of hundreds of large, new databases containing data rich in information that is of interest to many organisations.

The standard of data security in Australian organisations is low. Leaks will no doubt occur, as a result of accidents and errors. In addition, because the data is attractive, it will inevitably be subject to attacks. Even if security safeguards on these hundreds of databases is much improved, a proportion of these attacks will succeed. As explained in our primary submission, the APF is not satisfied that the existing, or proposed, legal safeguards on the security of such data are adequate.

(3) The proposal is that the Parliament delegate to the Executive infinite extensibility of access.

As the Bill stands, Parliament is being asked by the Executive to authorise the Executive to have ultimate determining power over the data that is to be collected, the agencies that are to have access to it, and the service providers subject to the retention obligation. The reliance, for key elements of the regime, on processes that do not involve full Parliamentary scrutiny, opens to the door to special pleading by a range of agencies. This is not merely incidental function creep, but appears to us to be designed-in function-creep. Accordingly, the APF submits that key elements establishing the scope of the regime should be set out in legislation, and not left to be determined by delegated legislation.

(4) Access is not subject to powerful regulatory control, but only to weak oversight agencies.

The suggestions made that existing safeguards – such as the IGIS, law enforcement integrity agencies, Ombudsman and Privacy Commissioner - represent effective protections for the public interest cannot be sustained. All such agencies are provided with limited powers, and extremely limited resources. In many instances, they have been unable to control excesses during the past; and their respective tasks would be complicated by the vast volumes of data mandated under a blanket data retention scheme. While the APF welcomes an increased role for the Ombudsman, we submit that this in no way sufficient for the privacy threats created by mass data retention.

Q4: We have been assured that data retention is the only effective way to address threats posed by criminal activities and threats to national security. Is this accurate?

APF's Response:

This proposition has not been substantiated by either independent studies or evidence presented to the Committee.

(1) The evidence relied upon is assertive, anecdotal, and far from comprehensive.

Good public policy should not be based on an uncritical acceptance of assertions or anecdotal evidence, important elements of which are not placed on the public record. The evidence presented to the Committee by law enforcement agencies implies that it may never be possible to evaluate the effectiveness of the use of metadata in criminal investigations. The APF rejects the proposition that assertions made by interested parties should be uncritically accepted; and then form the basis of public policy making. The APF considers that the public interest requires strong independent scrutiny of claims made in support of policies that would significantly erode the privacy of Australians; and that this Committee must provide that scrutiny.

(2) Insufficient attention has been given to counter-evidence.

As explained in our primary submission, in other jurisdictions, including the United States, independent bodies have found that some claims made in support of the effectiveness of the use metadata in investigations have not been entirely accurate. This suggests that there is considerable scope for the Committee to engage in more critical analysis in relation to both claims of the effectiveness of mass data retention, and the feasibility of alternative arrangements, than appears to have been the case to date. What we can say, however, is that on the basis of the limited evidence of the use of metadata that is on the public record, the evidence presented is not compelling.

Q5: Do you have any final comments?

APF's Response:

As explained in the APF's primary submission, the mandatory blanket retention of metadata has been rejected by every court that has reviewed such laws on the basis that it represents an invasion of privacy that is not justified by necessity or proportionality. In Australia, it is not possible to challenge the policy before the courts as there is no general judicial review on the grounds of infringements of fundamental human rights. It is therefore incumbent on Parliament, and Parliamentary committees, such as the PJCIS, to engage in thorough reviews of policies by an informed analysis of their impact on fundamental human rights. We therefore urge the Committee to fully take into account the decisions of eminent judicial bodies that have rejected blanket data retention, and the reasons for those decisions, in its deliberations on the proposals in the current Bill.

Thankyou for your consideration.

Australian
Privacy
Foundation

Attachment
APF's Meta-Principles for Privacy Protection

APF has worked on a wide variety of issues over more than a quarter-century. Its Policy Statements and its Submissions reflect the following set of ground rules, or meta-principles, which APF submits must be generally applied.

1. Evaluation
All proposals that have the potential to harm privacy must be subjected to prior evaluation against appropriate privacy principles.

2. Consultation
All evaluation processes must feature consultation processes with the affected public and their representative and advocacy organisations.

3. Transparency
Sufficient information must be disclosed in advance to enable meaningful and consultative evaluation processes to take place.

4. Justification
All privacy-intrusive aspects must be demonstrated to be necessary pre-conditions for the achievement of specific positive outcomes.

5. Proportionality
The benefits arising from all privacy-intrusive aspects must be demonstrated to be commensurate with their financial and other costs, and the risks that they give rise to.

6. Mitigation
Where privacy-intrusiveness cannot be avoided, mitigating measures must be conceived, implemented and sustained, in order to minimise the harm caused.

7. Controls
All privacy-intrusive aspects must be subject to controls, to ensure that practices reflect policies and procedures. Breaches must be subject to sanctions, and the sanctions must be applied.

8. Audit
All privacy-intrusive aspects and their associated justification, proportionality, transparency, mitigation measures and controls must be subject to review, periodically and when warranted.