UNCLASSIFIED

Australian Government
Australian Security Intelligence Organisation

Director-General of Security

21 January 2015
Our ref: A8863393

Mr Dan Tehan MP
Chair
Parliamentary Joint Committee on
Intelligence and Security
Parliament House
Canberra ACT 2600

Dear Mr Tehan,

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014: Supplementary Information

Thank you for the opportunity for ASIO to appear before the committee's opening hearings on 17 December as part of its inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the data retention bill). I support the evidence given to the committee by Ms Hartland and other ASIO officers during hearings.

As noted in our submission and evidence to the inquiry, historical communications data is a vital intelligence tool for protecting Australia and its people from threats to their security. Historical communications data has been instrumental in assisting ASIO to identify and map networks of individuals who would seek to hide their activities, to rule others out of investigation, and to prevent threats from developing into harm to the nation. This includes well known instances where mass casualty terrorist attacks have been thwarted as well as other matters where intelligence advice has prevented terrorism, espionage, and foreign interference.

ASIO supports the Government's data retention bill which implements the committee's 2012 recommendations and provides a regime that will provide for a consistent retention scheme across industry. The bill is directed at addressing the longstanding concerns of ASIO and law enforcement partners that we will 'go dark' in our efforts to understand individuals and networks involved in prejudicing Australia's national security and those engaged in serious criminality. However, the proposed two year retention period is very much a compromise

GPO Box 2176
Canberra City ACT 2601
Telephone: 02 6249 6299
Facsimile: 02 6257 4501

from ASIO's perspective – we would prefer a longer retention period to enable us to perform our statutory functions – but we recognise the policy balance to be struck between national security needs, privacy of the community, and industry regulation.

There were a number of matters arising from the December hearings which this letter responds to (see Annexure A). Please also find attached a declassified version of our submission for public release, including for uploading on the inquiry homepage. Sensitive operational matters have been removed from the submission to avoid prejudicing national security, as have personal details that would have an adverse effect on an individual's privacy. The submission outlines ASIO's approach to appropriately accessing and using historical telecommunications data, and the procedural and accountability mechanisms that apply. We hope that by addressing these issues we can dispel the misconceptions regarding ASIO's use of historical communications data.

In relation to the draft transcripts of the 17 December hearing, we have separately provided marked up amendments to the inquiry secretariat.

I understand you have scheduled more time to hear from the Attorney-General's Department, ASIO and the AFP on 30 January. I intend to appear and will be pleased to expand on any matters in ASIO's submission or respond to issues arising from other hearings. In the meantime, if any members of the committee require briefings, or have any queries regarding ASIO's submissions, we would be pleased to brief them and you can get in touch with my office to make the necessary arrangements.

Yours sincerely,

Duncan Lewis

Annexure A

ASIO's responses to matters arising from the 17 December hearing

Access

The committee asked for agency views on recommendations by the Parliamentary Joint Committee on Human Rights (PJCHR) in relation to limiting access as follows:

> 1.49 The committee therefore recommends that the bill, so as to avoid the disproportionate limitation on the right to privacy that would result from disclosing telecommunications data for the investigation of any offence, be amended to limit disclosure authorisation for existing data to where it is 'necessary' for the investigation of specified serious crimes, or categories of serious crimes.
>
> …
>
> 1.51 The committee therefore recommends that, to avoid the disproportionate limitation on the right to privacy that would result from data that is disclosed for an authorised purpose being used for an unrelated purpose, the bill be amended to restrict access to retained data on defined objective grounds, including:
> - where it is 'necessary' for investigations of specific serious crimes such as major indictable offences or specific serious threats; and
> - used only by the requesting agency for the purpose for which the request was made and for a defined period of time.

The PJCHR recognised the Telecommunications (Interception and Access) (TIA) Act provisions in relation to ASIO's access to historical communications data would be unchanged by the data retention bill, and anticipated ASIO's national security role would continue to require it to have access to such data. In making the recommendation in paragraph 1.51, the PJCHR noted the safeguards in the TIA Act but also expressed a concern that data collected for one purpose could be used for another unrelated purpose. The TIA Act, Australian Security Intelligence Organisation Act 1979 and Attorney-General's Guidelines presently regulate ASIO's use of personal information and sharing with other agencies and the data retention bill would not change this. It is likely there will be instances where historical communications data is sought in relation to a particular security matter and then becomes relevant to another security matter, as presently occurs. It would impede ASIO's effective pursuit of its functions to be further limited in this regard, noting that there are existing safeguards including the Inspector-General of Intelligence and Security (IGIS) who provides independent assurance to the Attorney-General, Parliament, and the community in relation to the legality and propriety of ASIO's activities.

The committee also asked for agency views on whether a legislative bar on non-government access historical telecommunications data would be problematic.

There would be no adverse effect on ASIO's ability to perform its statutory functions if access to historical communications data was restricted to government bodies.

Authorisation and costs

The committee sought further information at the hearing on reported comments by former Director-General of Security, Mr David Irvine, that he was supportive of a warrant to access historical communications data. As the Acting Director-General of Security, Ms Kerri Hartland advised the committee, Mr Irvine made the comments on 8 August 2014 during a joint press conference with Australian Federal Police Commissioner Andrew Colvin relating to data retention.

The full context of Mr Irvine's comments has not been given in media reports suggesting he supported a warrant for accessing communications data. Mr Irvine raised the straw man of a 'general' warrant for collection of communications data in support of ASIO's functions – such a scheme would not be a warrant. Mr Irvine went on to say that if a warrant were required for every single request ASIO's work would grind to a halt and Commissioner Colvin made the same point in relation to law enforcement operations. It has been, and remains, ASIO's consistent position that the present oversight and accountability mechanisms regulating access to historical communications data held by service providers are sufficient, including review by the independent IGIS, and that a warrant regime would significantly impede ASIO's operations.

Related, the committee was interested in any estimates that agencies could provide of the resourcing impost of a warranted access regime. Agencies presently pay service providers to access historical communications data. For example, in 2014 ASIO paid approximately $8M in costs and associated staffing infrastructure and anticipates that this figure would more than double if authorisation warrants were also required. This does not include on-costs related to the Attorney-General's Department reviewing ASIO's warrant requests (consistent with present practice), resourcing of the authority issuing the warrants (presently the Attorney-General), or oversight by the Office of theIGIS. There would also be a significant impact on operational agility and outcomes for ASIO and law enforcement partners dealing with national security and serious criminal matters given the reduction in timeliness and opportunity cost in deploying resources to the additional work associated with a warranted regime. It is just not practical. *Retention period*
The committee sought agency views on whether retention periods should be consistent across categories of historical communications data – between telephony and Internet Protocol (IP)-based data. In ASIO's experience the retention period for historical

communications data are variable across service providers as shown by the example retention periods in Table 1, broadly mapped against the proposed dataset. A more detailed breakdown is provided in **Annexure B**, which is classified for national security reasons.

Historical communications data –comparative range of retention		
Matters to which information must relate	**Telephony**	**Internet**
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	Up to 7 years (and longer)	90 days to 5 years
2. The source of a communication	6 weeks to 7 years 62 days to 7 years (for SMS)	0 days to 5 years
3. The destination of a communication		
4. The date, time and duration of a communication, or of its connection to a relevant service		
5. The type of communication or relevant service used in connection with a communication	Up to 7 years	90 days to 5 years

Table 1: Comparative ranges of retention by main service providers of historical communications data

The retention period for IP- based data is particularly volatile and in the majority of mobile broadband cases the communications data does not resolve to a transaction. Given in the near term all the historical communications data will be IP-based due to the uptake of IP-based technologies, it is important that the legislation remain technology neutral. Additionally, there should be a single retention period across the board, with a particular need to increase the retention period for IP-related data from present arrangements. Uniformity in retention periods is critical to allow the resolution of a transaction across the different network providers, indispensable in the more fragmented nature of IP-based technologies. The suggestion that there could be different retention periods reflects the position the data retention bill is seeking to move away from of inconsistencies between legacy telecommunications systems that kept everything (PSTN telephony) and new systems that ideally keep almost nothing (IP-based). Communications data that does not resolve to a transaction (which is where the technology is heading) is not of significant value to service providers but it can be to ASIO and law enforcement agencies. ASIO's core requirement is ongoing access to such data with a mandated retention period across industry that applies to a defined set of historic telecommunications data.

The committee asked for any information agencies could provide on the relative harms across categories of various economic, criminal, and national security matters. This is an important point. Matters that focus the attention of ASIO and other agencies in the national security community are persistent over time, even if the granular detail or the

ways they emerge might change (including with technology). For example, terrorism, communal violence, espionage and foreign interference are and have been enduring threats which are expected to persist, but the particular forms of cyber-enabled espionage and sectarian violence driven by globally connected diasporic communities are newer and enabled through changes in society's use of technologies.

Unanticipated – even anticipated but unpredictable – events driven by social, demographic and economic circumstance develop over time frames far in excess of two years. The Arab Spring, for example, was very much such an unanticipated event. When such events do occur, it is crucial that the national security community is able to rapidly and comprehensively respond and understand the individuals at the core of these events and where Australia's national interests may intersect with them. ASIO's ability to develop such understanding and provide advice to other agencies that mitigates the risk to Australia, its interests, and the community is contingent on the availability of information.

The harm of national security issues that run beyond two years is best considered in terms of Australia's sovereignty, territorial and border integrity, and economy. These compromises may be patiently cultivated over many years, even openly, until individuals are in positions able to act contrary to Australian interests or economic assets are more responsive to foreign interests than national ones. While inherently difficult to quantify because of the latent nature of clandestine foreign activities, the economic harms of unfettered espionage and foreign interference alone would be great – easily running into the hundreds of millions of dollars.

Likewise, the safety of Australians is not easily quantified or weighed against other threats and other national interests. Much of ASIO's counter-terrorism focus is on the disruption of onshore attacks, attack planning, radicalisation and recruitment. Many of these activities take place over extended periods well in excess of two years. Again, a comprehensive preventative response is driven by the availability of information.

Dataset and industry obligations

The committee was interested in how much detail should be included in the TIA Act or the regulations, and heard an industry view seeking more certainty through codification in the Act. From ASIO's perspective, operational agility and response are vital in this area. With this in mind, regulations are the better solution to operate in a dynamic security environment and provide flexibility to adapt to changes in society and technology. A serious counter-example to defining everything in primary legislation is the history of IMEI interception in Australia which took 10 years to achieve because it required change to the legislation. There was a technical solution available within months and, if it was open to make a regulatory change, it could have been adapted

for in faster time without this capability gap for interception agencies. Regulations also can be more technology-centric and lend currency to the intent of the Act.

The committee was interested in the value of inclusion of upload and download volumes in the dataset, and heard an industry view that this is data that would need to be created as it has no use from their perspective. This particular element of historical communications data is useful to security and law enforcement investigations because it allows us to identify leads to potential events (such as download of extremist material or exfiltration of privileged information), and is one tool we can use to focus investigative effort at individuals within groups.

The committee was also interested in obligations applying to community or free Wi-Fi services, such as those provided by Internet cafes. One trend in technology is the ability to access and synchronise communications applications and data across platforms. This is driven in part by the expansion of bandwidth meaning communications services that are 'always on' are shifting seamlessly to 'always on everywhere'. As such, being able to understand in national security matters the detail of the connectivity of an individual of interest – delivered through Wi-Fi services provided by carriers, businesses, local government and the community – will be critical. ASIO would argue against wide-scale exemption of Wi-Fi network access providers from data retention obligations. At minimum, identifying details of the device, the Wi-Fi point of connection and the date-time stamp of the connection should be retained.

PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

THE COMMITTEE HAS RECEIVED ANNEXURE B FROM THE AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION.

CONTENTS OF THIS DOCUMENT ARE CONFIDENTIAL TO THE COMMITTEE