WESTERN AUSTRALIA POLICE FORCE

OFFICE OF COMMISSIONER OF POLICE

POLICE HEADQUARTERS
6TH FLOOR
2 ADELAIDE TERRACE, EAST PERTH
WESTERN AUSTRALIA 6004
TELEPHONE : (08) 9222 1474

Your Ref:
Our Ref: fA1594584
Inquiries: commissioner@police.wa.gov.au

[redacted]
Inquiry Secretary
Parliamentary Joint Committee on Intelligence and Security
The Department of the House of Representatives
PO Box 6021
Parliament House
CANBERRA ACT 2600

BY EMAIL: pjcis@aph.gov.au

[redacted]

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY – SUBMISSION FOR THE REVIEW OF THE MANDATORY DATA RETENTION REGIME

Thank you for your email of 8 April 2019, inviting the Western Australia Police Force to make a submission into the review of the mandatory data retention regime proscribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

The WA Police Force is pleased to provide the following submission against each of the legislative areas of focus outlined in the Committee's Terms of Reference.

Continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill:

The changes in technology are two-fold. Firstly, the telecommunications technology available to consumers has resulted in an increased use of encrypted communications and greater access to, and uptake of, Wi-Fi in public locations. In addition, 5G is currently being rolled out across Australia.

Technological changes also influence the 'products' available to law enforcement from telecommunication carriers/providers. These products are not consistent or standardised across carriers. Providers are not obliged to update law enforcement with new products that become available, with jurisdictions discovering new services via inter-agency liaison. The advancement of technology (such as 5G) may result in metadata not covered under the retention scheme. Telecommunication providers may not retain or provide that metadata to law enforcement which will create losses in lines of enquiry which would otherwise be available.

Appropriateness of the dataset and retention period:

The metadata products supplied by telecommunication providers are not returned in standardised formats or content, making interpretation by analysts and investigators difficult. There is no requirement under the TIA Act for carriers to provide advice or instruction on how to 'read' or interpret the data.

There are two elements of retention, the period for the carrier and also for the law enforcement agency. A minimum two year retention period for telecommunication providers is essential, as serious criminal matters may be re-examined by law enforcement throughout the investigation, as well as new lines of inquiry emerging. The outcome of investigations where crimes may not be reported immediately are improved by having a two year minimum retention period.

The WA Police Force supports the ability for data obtained to be held as long as possible to support operational needs. There is currently no requirement for telecommunication providers to retain Visitor Location Register (VLR) data. Due to the increased nature of telecommunications being conducted through encrypted web applications, there is a decline in text messages and telephone calls. This is causing a decline in the usefulness of conventional call charge, reverse call charge and cell tower download metadata which is covered by the TIA Act. VLR data is now a more reliable way to further investigations as it does not rely on a call or text message being made to return data. Telstra does not provide this data due to its omission from the TIA Act. This is a significant loss of inquiry for law enforcement due to the size of the telecommunications market controlled by Telstra (the company controls 50% of the post-paid market).

The WA Police Force supports initiatives to improve legislation around Identity Verification Requirements for Prepaid Mobile Services. A large percentage of applications for authorisations under the TIA Act submitted by the WA Police Force are for services connected using false subscriber details, identity theft or deliberate variations to names to avoid detection.

Costs, including ongoing costs borne by service providers for compliance with the regime:

The costs for similar products vary greatly between telecommunication providers. The WA Police Force would support improved transparency and regulation of how providers calculate their charges and suggest periodic reviews, particularly in the wake of system automation.

Potential improvements to oversight, including in relation to journalist information warrants:

Information about persons within each jurisdiction appointed under section 6BD (issuing authorities for Journalist Information Warrants) and section 180X Public Interest Advocates (PIA) should be provided to the appropriate law enforcement agencies to minimise the risk of unauthorised persons being approached. The WA Police Force was not aware of the persons appointed under section 6BD, increasing the risk of unauthorised persons being approached to make the authorisation for a warrant.

Geographic factors should also be considered when appointing a PIA due to the isolated nature of some States, particularly Western Australia. The WA Police Force has previously used a PIA located in South Australia due to none being appointed in Western Australia, causing both costs and delays to the progress of the application.

Any regulations and determinations made under the regime:

Under section 182(4) of the TIA Act, law enforcement agencies are unable to use data accessed under missing person provisions (section 178A) for any other purpose than finding the missing person. If the missing person is discovered to be deceased, disclosure of the information is permissible under section 182(2A) but the provisions of 'use' under section 182(4) do not allow for the information to be used except for the purpose of finding the missing person. Due to the restrictiveness of the 'use' of this information, if the matter then leads to a homicide investigation, the data is unable to be 'used' for the purposes of the homicide investigation.

Law enforcement agencies are then forced to re-order that metadata under the correct section of the TIA Act (section 178) in order to use that data. This incurs a duplicate cost, which, in the case of cell tower metadata, can cost over a $1,000 and delay the investigation. If that data is past the retention period, the data could be lost to law enforcement, unless provisions are made to allow law enforcement to use data previously obtained.

In addition, WA Police Force officers are required to assist the Coroner with investigations. There are no provisions under the current legislation to make requests for telecommunications metadata to assist a Coroner's investigation. Meaning, officers must attempt to get a warrant under the *Coroners Act 1996* (WA) to obtain that data.

Number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security:

There have been some issues encountered with smaller telecommunication service providers being unaware of their obligations under the TIA Act for data retention and provision, as well as some who have refused to provide data.

There are currently two outstanding queries referred to the Department of Home Affairs for clarification. The first involves one provider which believes it is not a provider as defined under the TIA Act and is exempt from obligations to provide law enforcement companies with metadata and obligations under the mandatory retention scheme, so subsequently has refused to comply with a request under the TIA Act. The second involves a telecommunications provider which has provided its carrier services through a re-seller company located in Europe. The primary company referred the WA Police Force to the re-seller to obtain the data, and the re-seller has then refused to provide the data due to being outside Australian jurisdiction. This is now an issue of whether it is the responsibility of the primary provider to retain and provide metadata from its re-seller under the TIA Act or, whether the overseas company carries the obligation. The WA Police Force is currently awaiting a resolution for both of these referrals.

In both scenarios, there is a very real possibility that the data has not been retained and the WA Police Force has lost this line of inquiry.

The WA Police Force has not referred any complaints to the Commonwealth Inspector-General of Intelligence and Security.

Security requirements in relation to data stored under the regime, including in relation to data stored offshore:

The WA Police Force supports the records of requests made under the TIA Act being stored securely and the prevention of access to requests by third parties. Ideally, there should be a uniform security classification rating across all carriers.

Any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the *Telecommunications TIA Act 1997*:

The WA Police Force accesses 000 audio recordings from Telstra under section 286 of the *Telecommunications Act 1997*. Call charge records from 000 calls are still requested under the TIA Act. The WA Police Force also accesses metadata under a warrant provided by s33(3) of the *Coroners Act 1996* (WA) as the TIA Act does not make any provisions for access to data by police officers acting as Officers of the Coroner.

This has caused some issues with the release of metadata as telecommunications providers are reluctant to provide metadata outside the TIA Act. There are also agreements in place with Microsoft and Blackberry (offshore providers) coordinated through the Department of Home Affairs for access to their subscriber metadata.

Developments in international jurisdictions since the passage of the Bill:

The WA Police Force note the following legislation, agreements and rulings:

- The enactment of the *Clarifying Lawful Overseas' Use of Data Act* (CLOUD Act);
- Agreement between United Kingdom and United States of America (obtaining USA data under the CLOUD Act);
- Initial negotiations between Australia (Department of Home Affairs) and the USA regarding access to data;
- International (social and telecommunications industry) climate regarding CLOUD Act;
- Human rights court ruling against UK data surveillance methods;
- Human rights court ruling against the *Investigatory Powers Act 2016* (UK) (IP Act); and
- Inconsistencies between the IP Act and European Law identified by the High Court (UK).

Yours sincerely

[redacted]

COL BLANCH
ACTING COMMISSIONER OF POLICE

/ July 2019