Law Council
OF AUSTRALIA

Office of the President

19 February 2020

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Chair

Supplementary Submission: Review of the mandatory data retention regime

Thank you for the opportunity for Law Council representatives to appear before the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) as part of its review of the mandatory data retention regime (**the Inquiry**) on 7 February 2020.

During the course of the Law Council's appearance, the Law Council took a question on notice. This supplementary submission provides a response to the query from the Deputy Chair of the Committee, the Hon Anthony Byrne MP, as to whether the Law Council has a view on the absence in the data retention regime of a mandated time period after which law enforcement and intelligence agencies are required to destroy the telecommunications data that they acquire from telecommunications providers from authorised requests.

It is the view of the Law Council that the mandatory data retention regime should require law enforcement and intelligence agencies to de-identify or put beyond use in a timely manner telecommunications data containing personal information which is irrelevant to, or no longer needed by, the agency.[1] The Law Council recommends that information in relation to how telecommunications data is stored, encrypted and disposed of should be made available to the public so that there is greater transparency and public trust in these key requirements of the scheme.[2]

The Law Council submits that the retention and subsequent disposal of telecommunications data by law enforcement and intelligence agencies should achieve consistency with the Australian Privacy Principles (**APPs**) under the *Privacy Act 1988* (Cth). APP 11 requires APP entities to take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer required for any purpose for which the

[1] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (20 January 2015) 26 [124]; Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia. *Review of the Mandatory Data Retention Regime* (18 July 2019) 28 [115].
[2] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia. *Review of the Mandatory Data Retention Regime* (18 July 2019) 28 [116].

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639 • *Email* mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

personal information may be used or disclosed under the APPs unless such retention of information is authorised by an order of a court or tribunal.[3]

The requirements of APP 11 have also had the benefit of additional guidance from the Office of the Australian Information Commissioner (**Guidelines**).[4] The Guidelines specifically address matters such as when destruction or de-identification may be appropriate, factors to be considered in assessing what may be 'steps that are reasonable' in the circumstances and what amounts to putting the information beyond use.[5] The Guidelines are informed and can be supplemented by the Protective Security Policy Framework and the Australian Signals Directorate's Australian Government Information Security Manual.[6]

Further, in the consideration of the timeframes within which telecommunications data should be de-identified or disposed, the Law Council considers that the Committee could be assisted by having regard to the requirements surrounding the destruction of bodily fluids, fingerprints and DNA evidence collected in the course of a criminal investigation. For example, section 3ZK of the *Crimes Act 1914* (Cth) requires certain forensic evidence to be destroyed 'as soon as practicable' following acquittal of the person it relates or within 12 months if no criminal prosecution is commenced.

The Law Council also notes the concerns raised by the Commonwealth Ombudsman (**Ombudsman**) during the course of the Committee's review regarding the premature deletion of telecommunications data. The Ombudsman has noted that there have been instances where telecommunications data obtained under an authorisation has been destroyed before the Ombudsman is able to undertake certain oversight and investigatory procedures. In those instances, the Ombudsman was unable to assess whether the data was accessed and used by the agency in accordance with the requirements of the scope of lawful authorisation. The Ombudsman has noted that access to the authorisation, but not the data to which it relates, impedes the capacity for the Ombudsman to provide public assurance as to the legality of the use of retained telecommunications data. The Law Council submits that the mandatory data retention regime must allow the effective exercise of oversight inspection activities.

Thank you again for the opportunity to appear before the Committee and provide this supplementary submission. Please contact Dr Natasha Molt, Director of Policy, on (02) 6246 3754 or at natasha.molt@lawcouncil.asn.au in the first instance, if you require further information or clarification.

Yours sincerely

Pauline Wright
President

---

[3] *Privacy Act 1988* (Cth) sch 1 cl 11.2(d).
[4] Office of the Australian Information Commissioner, Australian Government, *Australian Privacy Principles Guidelines* (July 2019) <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/>.
[5] Ibid.
[6] Attorney-General's Department, Australian Government, *Protective Security Policy Framework* (2012) <https://www.protectivesecurity.gov.au/> and Australian Signal's Directorate, Australian Government, *Australian Government Information Security Manual* (February 2020) <https://www.cyber.gov.au/ism>