Australian Government
Office of the Australian Information Commissioner

# Review of the mandatory data retention regime

## Supplementary submission of the Office of the Australian Information Commissioner

oaic.gov.au

OAIC

# Contents

# Supplementary submission to the review of the mandatory data retention regime

1. Thank you for the opportunity for the Office of the Australian Information Commissioner (OAIC) to appear before the Parliamentary Joint Committee on Intelligence and Security (the Committee) on 7 February 2020 (Committee hearing) in relation to its review of the mandatory data retention regime (the regime).
2. At the hearing the Australian Information Commissioner and Privacy Commissioner (the Commissioner) referred to areas of possible law reform in addition to those set out in the OAIC's July 2019 submission to the Committee. In the interest of particularising those matters, the OAIC provides this supplementary submission to assist the Committee.
3. The following four matters are outlined below:
    - record keeping requirements for telecommunications service providers
    - evidence gathering powers for OAIC oversight
    - information sharing amongst regulators
    - data breach notification requirements for all regime participants.

## Record keeping requirements in the *Telecommunications Act 1997*

4. Section 306 of the *Telecommunications Act 1997* (Cth) (Telecommunications Act) sets out a requirement for telecommunications service providers to keep records of disclosures of telecommunications data to enforcement agencies. The information that these records must contain are specified in s 306(5) and include:
    - the name of the person making the disclosure
    - the date of the disclosure
    - the grounds for the disclosure (such as the legislative provision under which the disclosure is authorised)
    - any applicable authorisation under the *Telecommunications (Interception and Access) Act 1979* (TIA Act)
    - any other bodies involved in the request
    - the telecommunications service used.
5. Service providers are not required to keep records of information relating to the kinds of information included in a disclosure, such as the types of telecommunications data that were disclosed.
6. This means that the OAIC's inspections under section s 309 of the Telecommunications Act do not allow officers to consider whether only necessary personal information is being disclosed by service providers when responding to information requests from enforcement agencies.
7. Accordingly, the OAIC recommends that the Committee consider an amendment to s 306(5) of the Telecommunications Act that requires service providers to keep records relating to the kinds of information included in disclosures. Such an amendment could, for example, require

service providers to itemise the types of telecommunications data set out in s 187AA of the TIA Act that were disclosed.

8. The OAIC could then oversee the extent to which service providers comply with such a requirement, utilising the monitoring functions conferred by s 309 of the Telecommunications Act.

## Additional evidence gathering powers

9. The effectiveness of the OAIC's monitoring of service providers' compliance with record keeping and Privacy Act requirements would be enhanced by greater powers to compel the production of evidence.[1] In the *Privacy Act 1988* (Privacy Act), compulsive evidence gathering powers are enlivened only in relation to investigations,[2] and not in relation to other monitoring functions.[3]

10. The Committee may be aware that, in its response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry, the Australian Government has committed to a review of the Privacy Act. The abovementioned evidence gathering powers are among the changes the OAIC will be recommending to the government as part of that review. Nevertheless, the OAIC also asks that the Committee considers whether these changes would be suitable for earlier implementation as part of this review of the TIA Act, to further strengthen the OAIC's regulatory oversight.

## Information sharing

11. At the Committee hearing, the Commonwealth Ombudsman gave evidence about the desirability of oversight agencies exchanging information.[4] The Commissioner noted that in some circumstances the OAIC is prevented from sharing information with other regulators because of disclosure restrictions in the *Australian Information Commissioner Act 2010* (AIC Act).[5]

12. At the Committee hearing, the Ombudsman indicated that information sharing can help ensure appropriate oversight of all elements of the regime.

13. The OAIC agrees that oversight of the mandatory data retention regime would be improved if the oversight agencies involved were authorised to share intelligence on matters of regulatory concern where there is a public interest to do so. To that end, the OAIC asks that the Committee consider addressing this issue by amendments to s 29 of the AIC Act, and any other statutes that apply similar constraints on information sharing.

## Data breach notification in the context of the regime

14. The OAIC also wishes to draw to the Committee's attention to data breach notification in the context of the regime.

---

[1] Section 44 of the Privacy Act.

[2] Section 40 of the Privacy Act.

[3] While the privacy assessment (audits) power under s 33C of the Privacy Act provides discretion around the manner of conducting an assessment, my Office cannot compel the production of documents or enter premises without the consent of a participating entity.

[4] Evidence to the Parliamentary Joint Committee on Intelligence and Security, Canberra, 7 February 2020, Hansard p. 10-11, Mr Michael Manthorpe, Commonwealth Ombudsman.

[5] Refer to s 29.

15. In the time since the commencement of the regime, amendments to the Privacy Act introduced the Notifiable Data Breaches (NDB) scheme.[6] The Committee recommended the introduction of a mandatory data breach notification scheme in its 2015 advisory report.[7] The NDB scheme requires organisations to assess whether or not a data breach is likely to cause significant harm to those whose personal information has been compromised as a result of the breach, and provide notifications to the Commissioner and the affected individuals in the event that threshold is met.[8] Data breach notification is an important transparency measure that is present in many privacy regimes around the world.

16. All service providers with obligations under the regime are covered by the Privacy Act, and therefore also the NDB scheme, by virtue of s 187LA of the TIA Act. The Privacy Act and the NDB scheme also applies to Commonwealth enforcement agencies. However, State and Territory enforcement agencies[9] are not subject to the Privacy Act and there is no equivalent scheme for data breach notification in the States and Territories with privacy legislation.[10]

17. To address this regulatory gap, in the absence of State and Territories introducing NDB schemes, such agencies could be brought within the jurisdiction of the Privacy Act in relation to their collection and use of telecommunications data for the purposes of the regime.

18. One mechanism to achieve this could be to utilise s 6F of the Privacy Act, which allows a State or Territory agency to be prescribed as an 'organisation' in relation to specific acts or practices. This would assist in providing an enhanced and consistent level of privacy protection in relation to telecommunications data that is handled across Australia, noting that any currently exempted bodies such as intelligence agencies and exceptions in relation to 'enforcement' bodies and 'enforcement related activity' would not be affected.

19. In practice, this would mean that if a State or Territory agency suffered a notifiable data breach under the Privacy Act, those agencies would be required to notify the OAIC. The OAIC would then be in a position to offer advice and guidance in relation to the breach, which may include referring the matter to a State or Territory privacy regulator for further action if necessary.

20. Thank you for the opportunity to provide a supplementary submission to the Committee. The OAIC is available to provide further information or assistance to the Committee as required.

---

[6] Refer to Part IIIC of the Privacy Act.

[7] Refer to pp. 293-299; Recommendation 38.

[8] There are exceptions to the notification requirement in certain circumstances, including if the notification to affected individuals would be inconsistent with a Commonwealth secrecy provision or the notification would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body.

[9] State and territory police forces are criminal law-enforcement agencies for the purposes of the TIA Act under s 110A(1)(b).

[10] South Australia and Western Australia do not have legislation that addresses privacy. The remaining jurisdictions have privacy legislation.