Australian Government

Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report:

Review of the mandatory data retention regime

FEBRUARY 2023

Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report

Review of the mandatory data retention regime

Opening Comment

The Government thanks the Committee for its considered and comprehensive report on the mandatory data retention regime. The Government is committed to ensuring transparency and accountability of the regime and recognises the need to protect the privacy of Australians while also supporting law enforcement and national security agencies to effectively fulfil their important functions.

A proportionate and effective mandatory data retention regime is necessary to ensure our electronic surveillance laws are adapted to agencies' operational requirements, subject to appropriate safeguards. The regime supports restricted access to electronic information by law enforcement and national security agencies when needed to prevent, disrupt and investigate serious crimes and threats to national security.

Implementation of a number of the Committee's recommendations will require legislative reform. The Government will seek to progress these legislative amendments through appropriate legislative action.

Concurrently, the Government is developing holistic reforms to the Commonwealth electronic surveillance legislative framework in response to recommendations of the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Comprehensive Review). This includes aligning the statutory thresholds for access to electronic surveillance powers and ensuring appropriate privacy protections. As part of these reforms, the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) would be repealed and replaced by a single Bill that consolidates and aligns relevant provisions of the TIA Act, the *Surveillance Devices Act 2004* (Cth) and parts of the *Australian Security Intelligence Organisation Act 1979* (Cth).

The Government is consulting with industry and other stakeholders in designing the reforms to ensure the proposed settings are proportionate and effective, and that the regulatory burden is appropriate.

The Government provides the following responses to the Committee's recommendations on the mandatory data retention regime.

Recommendation One

Within 18 months from the date of the Committee's report, the Committee recommends that the Department of Home Affairs prepare national guidelines on the operation of the mandatory data retention scheme by enforcement agencies. In general terms, the purpose of the national guidelines would be to ensure greater clarity, consistency and security in respect of requests for – and the collection and management of – telecommunications data by enforcement agencies across Australia.

To that end, the national guidelines must be:

- consistent with the requirements of the *Telecommunications (Interception and Access) Act 1979* and other relevant Commonwealth legislation (as amended in accordance with the other recommendations made by the Committee in this report); and
- adopted and followed by each enforcement agency.

In developing the national guidelines, the Department of Home Affairs should meet and consult with (at a minimum):

- the Privacy Commissioner;
- the Commonwealth Ombudsman;
- each criminal law-enforcement agency;
- industry representatives;
- the Law Council of Australia; and
- the Department of Infrastructure, Transport, Regional Development and Communications.

The national guidelines should be made public (except to the extent they contain classified information, if any).

The Government accepts this recommendation

The Government agrees the operation and understanding of the mandatory data retention regime must be clear and consistent across telecommunications providers and agencies.

The Attorney-General's Department will publish Guidelines to assist agencies and providers applying the TIA Act. As well as addressing this recommendation, the Guidelines also respond to Recommendations 2, 3, 7 and 11.

As outlined in the Committee's report, the Guidelines reflect the necessity of protecting individual privacy and ensuring powers are applied consistently and proportionately across agencies, providers and oversight.

In developing the Guidelines, the Attorney-General's Department consulted Commonwealth, state and territory agencies and industry representatives through the Interception Consultative Committee. The department also consulted the Department of Infrastructure, Transport, Regional Development, Communications and the Arts; the Office of the Commonwealth Ombudsman; the Office of the Australian Information Commissioner; and the Law Council of Australia.

Through this consultative process, the Attorney-General's Department has ensured the Guidelines are consistent with the intent of the legislation, represent best practice (particularly around safeguards) and are able to be adopted and followed by agencies.

Separately, ASIO complies with the Minister's Guidelines, which provide safeguards and accountability for ASIO's use of the mandatory data retention regime. These Guidelines contain principles of proportionality governing the way ASIO obtains information, including that inquiries and investigations should be undertaken using as little intrusion into the privacy of affected individuals as is reasonably required, and that where possible, the least intrusive techniques for collecting information should be used before more intrusive techniques.

The Attorney-General's Department will ensure the Guidelines remain up to date, and will amend and release further Guidelines, in consultation with stakeholders, if additional areas requiring guidance are identified.

Recommendation Two

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to clearly define the term "content or substance of a communication" for the purpose of providing greater certainty and enhancing privacy protections.

The Department of Home Affairs should, at a minimum, meet and consult with the following in seeking to develop this definition:

- the Communications Alliance and other industry representatives;
- the Commonwealth Ombudsman;
- the Inspector-General of Intelligence and Security;
- the Law Council of Australia; and
- the Privacy Commissioner.

Moreover, in defining the term "content or substance of a communication", Home Affairs should specifically consider whether some information that is currently treated as telecommunications data should now be regarded as content given what that information can reveal about an individual.

The Government accepts this recommendation.

The Government agrees that the obligations on carriers and carriage service providers under the mandatory data retention regime should be clear, and should not extend to the contents or substance of a communication.

The Government also agrees that legislative amendments to provide greater clarity about what is considered to be 'content' and 'non-content' data for the purposes of the mandatory data retention regime would enhance privacy protections by reducing the potential for 'content' information to be inadvertently and unlawfully disclosed to agencies without a warrant.

The Government notes that inserting a legislative definition of 'contents or substance of a communication' in the TIA Act would have broader implications beyond the scope of the mandatory data retention regime, and affect the interpretation of provisions governing the use of electronic surveillance powers more broadly.

In addition to providing clarity and ensuring due protection for privacy, and consistent also with the recommendations of Mr Dennis Richardson AC in his Comprehensive Review[1], the statutory definition should aim to be technology neutral.

The Government will progress this recommendation through appropriate legislative action.

In the interim, prior to legislative reform, the Attorney-General's Department will issue additional guidance for agencies and industry on what is the 'content or substance of a communication'. The guidance will be developed in consultation with agencies, industry and oversight agencies including Commonwealth, state and territory agencies and industry representatives through the Interception Consultative Committee; the Department of Infrastructure, Transport, Regional Development, Communications and the Arts; the Office of the Commonwealth Ombudsman; the Office of the Inspector-General of Intelligence and Security; the Office of the Australian Information Commissioner; and the Law Council of Australia.

Recommendation Three

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended so that, if a provider discloses any of the information referred to in section 187A(4) of the *Telecommunications (Interception and Access) Act 1979* to ASIO or a criminal law-enforcement agency, ASIO or the enforcement agency (as applicable) must:

- not use the information;
- immediately quarantine the information;
- notify the Commonwealth Ombudsman or the IGIS (as applicable) of the disclosure; and
- following consultation with the Ombudsman or the IGIS (as applicable), destroy the information.

The Government accepts this recommendation.

The Government agrees that agencies that receive information that should not have been disclosed to them should not be able to use that information. In particular, quarantine and notification obligations should apply if agencies unintentionally receive the contents or substance of a communication.

The Government will progress this recommendation through appropriate legislative action.

Agencies in practice already quarantine and delete the contents or substance of a communication and web-browsing history if the agency identifies this information as having been supplied by a service provider in error. The Government will introduce legislative amendments to impose these practices as statutory obligations on agencies.

In the interim, prior to legislative reform, the Attorney-General's Department will also issue additional guidance for agencies on how content information should be quarantined and destroyed if it is received in error.

[1] https://www.ag.gov.au/national-security/consultations/comprehensive-review-legal-framework-governing-national-intelligence-community

The Government notes that agencies may have practical difficulties in determining whether information they receive falls within subsection 187A(4) of the TIA Act. The Guidelines and updated legislation will take this into account.

Recommendation Four

The Committee recommends that the data retention period be kept at two years.

The Government accepts this recommendation.

Recommendation Five

The Committee recommends that section 187A of the *Telecommunications (Interception and Access) Act 1979* be amended to clarify that service providers are not required to store information generated by Internet of Things devices.

The Government accepts this recommendation.

The Government is committed to protecting the privacy of Australians while ensuring agencies can access the information they need to protect community safety. The Government agrees that a general requirement for service providers to retain data generated by all Internet of Things devices would not be appropriate given the wide range of devices and the potentially significant compliance costs for service providers.

Defining Internet of Things devices and communications and delineating them from more traditional devices is a complex task. Devices such as internet-connected vehicles and smart-watches could be considered Internet of Things devices, and the data they generate is analogous in some respects to data generated by mobile phones (for example, location data). This data can be crucial for agencies tasked with preventing, deterring and combatting serious crime and threats to national security.

Recognising this, the Committee's view was that if the Government considers there are clear benefits in requiring service providers to keep information for *particular* Internet of Things devices, and that those benefits outweigh the costs, the TIA Act could be further amended to impose clear and specific requirements on providers to retain information.

Defining Internet of Things devices would also require consideration of other key definitions and concepts underpinning the TIA Act, such as the definition of *communication*.

The Government will consider in detail the treatment of Internet of Things devices when designing its holistic reforms of the electronic surveillance legislative framework.

Recommendation Six

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to include the following additional reporting requirements:

- the number of authorised officers in each enforcement agency and ASIO;
- the number of authorisations made by each authorised officer;
- the number of individuals that the authorisations by each enforcement agency and ASIO related to; and

- in respect of authorisations in relation to criminal investigations, the specific offence – or offences – that the authorisations related to.

The Government accepts this recommendation in principle.

The Government considers that agency reporting is fundamental to the transparency and accountability of the use of powers under the *Telecommunications (Interception and Access) Act 1979*.

The Government agrees with the Committee that increased agency reporting on the operation of the mandatory data retention framework could assist oversight and review bodies in undertaking their work, provide a higher degree of transparency and give the Parliament and the Australian community greater trust in the use of these powers. The Government will progress practicable and meaningful reforms to the reporting framework to better enable oversight.

The Government will develop enhanced reporting requirements through appropriate legislative action. In the interim, prior to legislative reform, the Attorney-General's Department will seek additional information from enforcement agencies for inclusion in the 2022-23 *Telecommunications (Interception and Access) Act 1979* Annual Report.

To achieve the intent of this recommendation, it may be necessary for agencies to update information systems to capture the required information and generate reporting and to update training for authorised officers. Given that enforcement agencies and ASIO have different operating models and oversight arrangements, different approaches may be required to meet the intent of the recommendation.

Consistent with agencies' current practices for reporting, careful consideration will be required to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed.

The current distinction between reporting for law enforcement agencies and reporting for ASIO will be maintained. The Government notes that ASIO is also subject to additional oversight and reporting requirements.

Recommendation Seven

The Committee recommends that, in consultation with other stakeholders (agencies with access to the Mandatory Data Retention Regime, the Inspector General of Intelligence and Security, the Commonwealth Ombudsman and the Commonwealth Privacy Commissioner), the Department of Home Affairs should within 18 months of this report develop guidelines for data collection to be applied across the Mandatory Data Retention Regime and the most cost effective way to achieve the intended outcome of facilitating better oversight, including an ability for enforcement agencies and Home Affairs to produce reports to oversight agencies or Parliament when requested.

As a minimum, any such report should include the following information (in respect of each occasion on which the powers in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* were used):

- the section of the *Telecommunications (Interception and Access) Act 1979* used to access the data;
- the case number associated with the authorisation;
- the specific offence – or offences – that the investigation related to;
- if the authorisation related to a missing person case, the name of the missing person
- brief reasons why the authorised officer was satisfied that the disclosure was reasonably necessary;
- where the data related to a person who did not have an obvious relationship to a suspect in an investigation, brief reasons why the authorised officer was satisfied that any interference with the privacy of the person that may have resulted from the disclosure or use of the telecommunications data was justifiable and proportionate;
- the name(s) of the officers involved in the case;
- the name and appointment of the authorising officer;
- if the agency became aware that the carrier disclosed any of the information referred to in section 187A(4) and action taken.

Where practicable, the report should also include:

- whether or not the data was used to rule someone out from an investigation;
- whether or not the person whose data was accessed was eventually charged, prosecuted and/or convicted of a crime;
- whether or not the data accessed eventually led to the charge, prosecution and/or conviction of another person for a crime; and
- the cost of the disclosure.

For the Australian Security Intelligence Organisation, the additional record-keeping requirements should include:

- the nature of the national security risk that led to the authorisation being given; and
- brief reasons why the authorised officer is satisfied that any interference with the privacy of the person that may result from the disclosure or use of the telecommunications data is justifiable and proportionate.

The Government accepts this recommendation.

The Government shares the Committee's concerns about the absence of consolidated data on the operation of the mandatory data retention regime.

The Government agrees with the Committee that collecting more information about the current functioning of the data retention regime will assist oversight and review bodies in undertaking their work, provide a higher degree of transparency and give the Parliament and the Australian community greater assurance about the use of these powers.

The Government agrees to providing greater guidance to ensure agencies keep sufficient and consistent information to be able to assure Parliament and oversight agencies that access and use of telecommunications data is lawful and appropriate. The Attorney-General's Department will develop guidance, in consultation with agencies, industry and oversight agencies, in line with the response to recommendation 1.

Consistent with agencies' current practices for reporting, careful consideration will be required to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed. The current distinction between reporting for law enforcement agencies and reporting for ASIO will also need to be maintained.

In addition, the Government will further consider reporting requirements as part of holistic reforms to electronic surveillance legislation. This will ensure that reporting and oversight across the entirety of the electronic surveillance framework is considered and the totality of information captured by agencies against each warrant or authorisation allows for effective and efficient oversight, while not placing an undue burden on agencies.

Recommendation Eight

The Committee recommends that section 306(5) of the *Telecommunications Act 1997* be amended to require telecommunications service providers to keep detailed records of the kinds of information included in each disclosure of telecommunications data, including the types of telecommunications data that were disclosed.

The Government accepts this recommendation.

The Government supports changing the record-keeping requirements in subsection 306(5) of the *Telecommunications Act 1997* and has introduced legislative amendments to this effect in the Telecommunications Legislation Amendment (Information Disclosure, National Interest and Other Measures) Bill 2022.

The Government also introduced amendments to existing record-keeping obligations to provide more clarity and transparency on the underlying legislative provisions that authorise a disclosure of information through section 280 of the *Telecommunications Act 1997*. These amendments will assist the Office of the Australian Information Commissioner in its compliance monitoring of such records as set out in section 309 of the *Telecommunications Act 1997*.

The Department of Infrastructure, Transport, Regional Development and Communications and the Arts will lead implementation of this recommendation.

Recommendation Nine

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended so that:

- ASIO and enforcement agencies are required to retain telecommunications data for a prescribed minimum period to ensure that the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman (as applicable) are able to perform their oversight functions; and
- Having satisfied the requirements of the Inspector-General of Intelligence and Security or the Commonwealth Ombudsman (as applicable) ASIO and enforcement agencies are required to delete telecommunications data as soon as practicable after the telecommunications data is no longer needed (e.g. in the case of an enforcement agency, after an investigation has concluded).

The Government accepts this recommendation

Independent oversight by the IGIS and the Commonwealth Ombudsman is fundamental to ensuring accountability in the operation of the mandatory data retention regime. The Government agrees that this oversight role must be adequately supported and facilitated by agencies' record keeping practices.

The Government will progress this recommendation through appropriate legislative action. In designing these reforms, the Government will work with oversight agencies to ensure record keeping and destruction requirements appropriately address privacy considerations, effective oversight and operational requirements.

The Government notes the Minister's Guidelines to ASIO require the Organisation to take reasonable steps to destroy or otherwise dispose of personal information, where that information is no longer required for the performance of the Organisation's functions, or to demonstrate compliance with the laws of the Commonwealth and of the States and Territories.

The Government also notes particular work will be required to determine the circumstances in which data is no longer required by enforcement agencies. Implementation of this recommendation may also require significant change in systems and practice by agencies.

The Attorney-General's Department, in consultation with the Department of Home Affairs, will progress action on this recommendation.

Recommendation Ten

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended so that:

- authorised officers may only make verbal authorisations for the disclosure of telecommunications data in emergency situations; and
- the record-keeping obligations that apply to written authorisations also apply to verbal authorisations except that:
    - the written record must be made as soon as practicable after the making of the verbal authorisation; and
    - for each verbal authorisation, the authorised officer must make a record of the reasons why the authorisation had to be made verbally.

The Government accepts this recommendation.

The Government will progress this recommendation through appropriate legislative action.

The Attorney-General's Department will lead the implementation of this recommendation, in consultation with oversight agencies.

Recommendation Eleven

The Committee recommends that section 5AB of the *Telecommunications (Interception and Access) Act 1979* be amended with a view to reducing the number of officers and officials of criminal law-enforcement agencies who may be designated as "authorised officers" and the circumstances in which those designations may be made. At a minimum:

- only officers or officials who hold a supervisory role in the functional command chain should normally be capable of being designated as 'authorised officers'; although
- other individuals who hold specific appointments – rather than entire classes of officers or officials – may be capable of being designated as 'authorised officers';
- in order to authorise an individual to be an authorised officer, the head of an enforcement agency must be satisfied that it is necessary for the individual to be an 'authorised officer' in order for the individual to carry out his or her normal duties; and
- prior to the head of an enforcement agency authorising an individual to be an 'authorised officer':
    - the relevant senior officer or official must complete a compulsory training program in relation to Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*; and
    - the head of the enforcement agency must be satisfied that the senior or official has the requisite experience, knowledge and skills to exercise the powers under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*.

The Government accepts this recommendation.

Authorised officers play a critical role in the operation of the electronic surveillance framework. The Government shares the Committee's concerns about ensuring authorised officers are appropriately trained and agrees that there are potential benefits in ensuring a more consistent national approach to the training, qualifications and experience of officers designated as "authorised officers" for the purposes of the TIA Act.

Through the development of the holistic electronic surveillance reforms, the Government will carefully consider an appropriate threshold that the chief officer of each agency must be satisfied of in order to designate particular officers, or individuals occupying specified positions, as authorised officers. This threshold will be prescribed in legislation.

In designing this threshold, the Government will enable agencies to maintain a sufficient number of authorised officers who are appropriately trained and experienced to ensure both operational effectiveness and due consideration of each authorisation decision.

In the interim, the Attorney-General's Department has developed Guidelines for use by agencies when considering the designation of authorised officers under the TIA Act. The Guidelines provide agencies with assistance in ensuring a sufficient number of authorised officers are available with the appropriate seniority, training and expertise.

Recommendation Twelve

The Committee recommends that section 180 of the *Telecommunications (Interception and Access) Act 1979* be amended to specify when a revocation of an authorisation takes effect.

The Government accepts this recommendation.

The Government will progress this recommendation through appropriate legislative action.

The Attorney-General's Department will lead the implementation of this recommendation.

Recommendation Thirteen

The Committee recommends that section 178 be amended and section 179 be repealed so that an authorised officer cannot make an authorisation for access to existing information or documents unless he or she is satisfied that the disclosure is reasonably necessary for:

- the investigation of:
    - a serious offence; or
    - an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

For the avoidance of doubt 'serious offence' is as defined in section 5D of the *Telecommunications (Interception and Access) Act 1979*.

The Government accepts this recommendation in principle.

The Government is committed to ensuring access to telecommunications data is necessary and proportionate, and recognises the Committee's concerns about the scope of agencies' ability to access telecommunications data.

The Government, through its work on the holistic electronic surveillance reforms, is considering the thresholds that should be met by law enforcement agencies seeking to conduct activities in order to access telecommunications information. The Government will propose legislative reforms that ensure thresholds are appropriate across the range of activities agencies are able to undertake to access this information.

Recommendation Fourteen

The Committee recommends that Division 3 of Part 4–1 of the *Telecommunications (Interception and Access) Act 1979* be amended to:

- increase the threshold for ASIO to authorise the disclosure of telecommunications data so that it is consistent with the threshold for ASIO to intercept telecommunications or access stored communications under a telecommunications service warrant issued under Part 2–2 of the Act; and
- introduce a new provision, modelled on section 180F of the *Telecommunications (Interception and Access) Act 1979*, requiring ASIO to consider privacy before making an authorisation.

The Government accepts this recommendation in part.

The Government appreciates the Committee's concerns about the privacy impacts of access to telecommunications data and notes the IGIS's observations about the current threshold. The Government agrees that agencies' powers should go no further than necessary to carry out their functions, and access to telecommunications data should be limited to that which is necessary and proportionate.

Restricted access to telecommunications data as recommended by the Committee would be a fundamental change to ASIO's operations and would significantly constrain ASIO's capability to protect Australia and Australians from threats to their security.

Recommendation Fifteen

The Committee recommends that section 280(1)(b) of the *Telecommunications Act 1997* be repealed.

Moreover, the Committee recommends that the Government introduce any additional amendments to Commonwealth legislation that are necessary to ensure that:

- only ASIO and the agencies listed in section 110A of the *Telecommunications (Interception and Access) Act 1979* be permitted to authorise the disclosure of telecommunications data; and
- those agencies can only access telecommunications data through Part 4–1 of the *Telecommunications (Interception and Access) Act 1979* and through no other legal mechanism.

The Government accepts this recommendation in principle.

The Government shares the Committee's concerns that paragraph 280(1)(b) of the *Telecommunications Act 1997* can operate as an inappropriate means to access telecommunications data without appropriate oversight and safeguards.

The Government will introduce legislation to repeal this provision and replace it with one that limits access to data (including personal information of subscribers) to specified entities in situations where that access is necessary and proportionate to achieving an allowable purpose. This will include consideration of reforms to other relevant provisions of the *Telecommunications Act 1997* as required. These reforms will address the need to protect the personal information of subscribers and manage regulatory costs to industry.

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts will progress action on this recommendation.

Recommendation Sixteen

The Committee recommends that sections 186 and 187P of the *Telecommunications (Interception and Access) Act 1979* be amended so that:

- the Minister must complete the report(s) referred to in section 186(2) and 187P as soon as practicable and, in any event, within 3 months after each 30 June; and
- the Minister must cause a copy of the report(s) to be tabled in each House of the Parliament as soon as practicable and, in any event, within 15 sitting days after the date on which the report is completed.

The Government accepts this recommendation in principle.

As noted in relation to recommendation 6, the Government views reporting as a fundamental aspect of the mandatory data retention regime, guaranteeing transparency and accountability over how agencies use their intrusive powers. Reports that are not provided to the Parliament and made public in a timely manner do not provide that transparency and accountability.

Reporting arrangements require the consolidation of data from law enforcement agencies in every jurisdiction in Australia. Agencies need a reasonable amount of time to prepare and check

data before providing it to the Attorney-General for consolidation. The Attorney-General's Department also undertakes a quality assurance process with each agency to ensure data is accurate and consistent across all agencies.

Further, the Australian Communications and Media Authority (ACMA) has the ability to compel information on compliance costs from service providers under the *Telecommunications Act 1997*, and then provides this to the Attorney-General's Department for inclusion in the TIA Act Annual Report, ordinarily 4-5 months after the end of each financial year. The Government will consider, through the holistic electronic surveillance reforms, providing another avenue for ACMA to report on this information, and if so, will repeal the requirement for this information to be included in the TIA Act Annual Report to allow for a faster tabling timeframe.

The Attorney-General's Department will work closely with agencies and ACMA to prepare TIA Act annual reports as quickly as possible.

The Attorney-General's Department will progress action on this recommendation.

Recommendation Seventeen

The Committee recommends that state and territory criminal law-enforcement agencies under section 110A be prescribed as 'organisations' under section 6F of the *Privacy Act 1988* in relation to their collection and use of telecommunications data for the purposes of the Notifiable Data Breach regime.

The Government notes this recommendation.

The Government supports the intent of the recommendation.

The Government believes that agencies that access telecommunications data under the mandatory data retention regime should be required to report when personal information is accessed or disclosed without authorisation, or is lost. This is an important safeguard that will build public confidence in the mandatory data retention regime and agencies' handling and use of personal information.

The ability to prescribe a state or territory law enforcement agency under the *Privacy Act 1988* requires the Commonwealth Attorney-General to be satisfied that the relevant state or territory has requested the prescription of that agency.

State and territory enforcement agencies are currently subject to oversight by state and territory oversight and privacy regulators. Any extension of the jurisdiction of the Office of the Australian Information Commissioner (OAIC) to state and territory agencies would require close consultation with the states and territories, and careful consideration of the interaction between the roles and responsibilities of the OAIC and state and territory oversight and privacy regulators to avoid duplication.

The Attorney-General's Department is leading a review of the *Privacy Act 1988*, which is expected to be completed by the end of 2022. The report will be released publicly following consideration by the Government.

The Attorney-General's Department will progress action on this recommendation in consultation with the OAIC, state and territory governments, criminal law-enforcement agencies and oversight and privacy regulators.

Recommendation Eighteen

The Committee recommends that section 182(2) of the *Telecommunications (Interception and Access) Act 1979* be amended in line with section 68(d) for the consideration of the communication of telecommunications data for disciplinary action and termination of employment.

The Government accepts this recommendation.

The Government will progress this recommendation through appropriate legislative action.

The Attorney-General's Department will lead the implementation of this recommendation.

Recommendation Nineteen

The Committee recommends that section 29 of the *Australian Information Commissioner Act 2010*, and any other statutes that apply similar constraints on information sharing by relevant oversight agencies, be amended so that agencies that have an oversight function in respect of the mandatory data retention regime are able to share intelligence on matters of regulatory concern where there is a public interest in doing so.

The Government accepts this recommendation.

The Government will progress this recommendation through appropriate legislative action. The Government notes the Privacy (Enforcement and Other Measures) Bill 2022 introduced in October 2022 enhances the Office of the Australian Information Commissioner's ability to share information with other regulators.

The Attorney-General's Department will lead the implementation of this recommendation.

Recommendation Twenty

The Committee recommends that the *Intelligence Services Act 2001* and the *Telecommunications (Interception and Access) Act 1979* be amended so that the Committee may commence a review of the mandatory data retention scheme by June 2025.

The Government accepts this recommendation.

The Government will implement this recommendation through appropriate legislative action.

The Attorney-General's Department will lead the implementation, in consultation with the Department of Home Affairs and the Department of Foreign Affairs and Trade.

Recommendation Twenty One

The Committee recommends that Division 1 of Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* be amended to require service providers to store

information of the kind specified in or under section 187AA, or documents containing information of that kind, on servers located in Australia unless specifically exempted.

The Government accepts this recommendation in principle.

The Government will implement this recommendation through appropriate legislative action.

The design of these reforms will require further consultation to fully determine the potential burden on industry; and with relevant agencies to ensure the Committee's intent of keeping data secure is met in the most appropriate manner.

The Attorney-General's Department will lead the implementation of this recommendation.

Recommendation Twenty Two

The Committee recommends that:

- agencies that have access to telecommunications data should develop minimum standards for the security of telecommunications data held within their control or premises; and,
- entities subject to telecommunications data retention requirements under the *Telecommunications (Interception and Access) Act 1979* should be required to demonstrate to the Australian Communications and Media Authority that they have met minimum standards for ensuring the security of retained data:
    - these minimum standards, applying to entities subject to telecommunications data retention requirements should be developed by the Australian Communications and Media Authority.

The Government accepts this recommendation in principle.

The Government agrees with the Committee that data retained by agencies and telecommunications providers should be subject to minimum security standards.

The Government notes the range of protections that already apply to data, including through the *Privacy Act 1988*, the TIA Act and the security obligations in the Telecommunications Sector Security Reforms.

In addition to the Attorney-General's Department's review of the *Privacy Act 1988*, the Department of Home Affairs is developing a national data security action plan as part of the new cyber security strategy, to deliver whole-of-economy expectations and requirements for data security.

The Attorney-General's Department will work with ACMA, the Department of Home Affairs, security and law enforcement agencies and oversight agencies to determine how minimum standards should be set in light of existing protections and planned reforms. The Attorney-General's Department will also consult with providers to ensure full consideration is given to the potential burden on industry.