2013-2014-2015

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2014

REPLACEMENT EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, Senator the Honourable George Brandis QC)

THE MEMORANDUM REPLACES THE EXPANATORY MEMORANDUM
PRESENTED TO THE HOUSE ON 30 OCTOBER 2014

TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2014

GENERAL OUTLINE

1. The last fifteen years have seen significant advancements in communications technology and changes to industry structure, practices and consumer behaviour. While the tools available to national security and law enforcement agencies in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) have been extremely successful in investigating, prosecuting and preventing serious criminal offences (including murder, sexual assault, kidnapping, drug trafficking, money laundering and fraud) and activities that threaten national security, the value of these tools is being undermined by the level of change in the telecommunications environment.

2. Serious and organised criminals and persons seeking to harm Australia's national security, routinely use telecommunications service providers and communications technology to plan and to carry out their activities. Some activities, including child pornography, are predominantly executed through communications devices such as phones and computers. The TIA Act provides a framework for national security and law enforcement agencies to access the information held by communications providers that agencies need to investigate criminal offences and other activities that threaten safety and security.

3. A critical tool available under the TIA Act is access to telecommunications data. Telecommunications data is information about a communication, such as the phone numbers of the people who called each other, how long they talked to each other, the email address from which a message was sent and the time the message was sent. Data is often the first source of lead information for further investigations, helping to eliminate potential suspects and to support applications for more privacy intrusive investigative tools including search warrants and interception warrants.

4. The global nature of the telecommunications industry and market and the development and growth of new technologies have created a rapid increase in new telecommunications services, changed business practices (including subscription rather than transaction based billing) and encouraged the adoption of new corporate models. All of these factors are diminishing traditional business requirements for retaining telecommunications data.

5. Currently, the TIA Act does not specify any types of data the telecommunications industry should retain for law enforcement and national security purposes or how long that information should be held. In lieu of any standardisation, individual carriers retain information based on business, taxation, billing and marketing requirements. This means there are significant variations across the telecommunications industry in the types of data available to law enforcement and national security agencies and the period of time that information is available. Agencies have publicly identified the lack of availability of data as a key and growing impediment to the ability to investigate and to prosecute serious offences.

6. On 24 June 2013 the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) handed down its report entitled *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. As part of that Inquiry the Committee considered

whether a mandatory data retention scheme should be introduced. In the Inquiry Report the PJCIS noted a diversity of views amongst Committee members and made several recommendations about what a mandatory data scheme should include if implemented. The Committee also made a number of recommendations about other aspects of the TIA Act.

7. The Bill will give effect to several of the PJCIS' recommendations including:

- Mandatory data retention will only apply to telecommunications data (not content) and internet browsing is explicitly excluded (Recommendation 42)
- Mandatory data retention will be reviewed by the PJCIS three years after its commencement (Recommendation 42)
- The Commonwealth Ombudsman will oversight the mandatory data retention scheme and more broadly the exercise of law enforcement agencies' exercise of powers under Chapters 3 and 4 of the TIA Act (Recommendations 4 and 42), and
- Confining agencies' use of, and access to, telecommunications data through refined access arrangements, including a ministerial declaration scheme based on demonstrated investigative or operational need (Recommendation 5).

8. This Bill will amend the TIA Act to standardise the types of telecommunications data that service providers must retain under the TIA Act and the period of time for which that information must be held.

9. Accessing content, or the substance of a communication (for instance, the message written in an email, the discussion between two parties to a phone call, the subject line of an email or a private social media post), without the knowledge of the person making the communication is highly privacy intrusive and, under the TIA Act, can only occur under an interception or stored communications warrant, or in limited other circumstances such as in a life-threatening emergency. Interception is subject to significant limitations, oversight and reporting obligations. None of these arrangements are affected by this Bill.

10. While telecommunications data is less privacy intrusive than content, law enforcement and national security agencies can only access data where a case can be made that this information is reasonably necessary to an investigation. This Bill will further strengthen privacy protections in the TIA Act in relation to data by limiting the types of enforcement agencies that can access telecommunications data.

11. Currently any authority or body that enforces a criminal law, a law imposing a pecuniary penalty or a law that protects the public revenue is an 'enforcement agency' under the TIA Act and can seek telecommunications data where that access complies with the requirements set out in Chapter 4 of the TIA Act. In 2012-13 data was accessed by around 80 Commonwealth, State and Territory agencies with law enforcement or revenue protection functions.

12. The Bill will require that bodies who are not a 'criminal law enforcement agency' for the purposes of the TIA Act must be declared by the Minister to be an 'enforcement agency' before they can authorise the disclosure of telecommunications data. These amendments will ensure that only authorities and bodies with a demonstrated need to have telecommunications information can authorise the disclosure of this information. These

amendments are consistent with Recommendation 5 of the PJCIS Report that the number of agencies able to access telecommunications data be reduced.

13. The Bill will further enhance privacy protections by introducing an independent oversight mechanism for access to data by law enforcement agencies. Under these provisions the Commonwealth Ombudsman will, for the first time, have the power to inspect the records of enforcement agencies to ensure that agencies are complying with their obligations under the TIA Act. The Inspector-General of Intelligence and Security (IGIS) currently oversights and, will continue to oversight, access to telecommunications data by the Australian Security Intelligence Organisation (ASIO).

14. The Bill will also amend Chapter 3 of the TIA Act to limit the availability of stored communications warrants in Part 3-3 of the TIA Act to a 'criminal law-enforcement agency'. Currently, any authority or body that is an 'enforcement agency' can apply for a stored communications warrant under Part 3-3. The Bill will limit this power to interception agencies and other law enforcement agencies with a demonstrated need for such information. A restricted definition recognises that text messages and emails stored on a phone or other communications device are more akin to content than data and should be subject to greater privacy protection than telecommunications data.

FINANCIAL IMPACT

15. The Bill will have financial impacts on service providers who will be required to meet the new minimum data retention obligations. A sample of affected service providers that cover the vast majority of services offered in Australia were consulted on the development of the policy and the regulatory impacts of the Bill.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

16. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

17. The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Bill) will amend the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and the *Telecommunications Act 1997* (Telecommunications Act) to introduce a statutory obligation for telecommunications service providers to retain for two years telecommunications data prescribed by regulations.

18. The proposed data retention obligation will require telecommunications service providers to retain prescribed telecommunications data, being information about a communication, as distinct from its content. The Bill will amend the TIA Act to prescribe the types of telecommunications data that may be prescribed by regulation for the purposes of the data retention obligation.

19. Telecommunications data, including subscriber information, is currently kept by service providers for billing, quality assurance and other business purposes. However, the evolution of business models associated with Internet Protocol (IP) convergence has led to less telecommunications data being created by and/or held on service provider systems. Consequently, there is an associated decrease in the availability of certain types of information that would assist law enforcement and intelligence agencies with their investigations.

20. The purpose of the Bill is to require service providers to retain a strictly defined subset of telecommunications data produced in the course of providing telecommunications services. This will ensure the availability of a specified range of basic telecommunications data for law enforcement and national security purposes. Telecommunications data is central to virtually every counter-terrorism, organised crime, counter-espionage and cyber-security investigation, as well as almost every serious criminal investigation, such as murder, rape and kidnapping. Telecommunications data is increasingly important to Australia's law enforcement and national security agencies, allowing agencies to determine how and with whom a person has been communicating. Access to telecommunications data also infringes less on personal privacy compared to other covert investigative methods as it does not include the content or substance of the communication.

21. Access to telecommunications data has proven to be a critical tool for security and law enforcement agencies, providing both intelligence and evidence when identifying and prosecuting offenders. Telecommunications data provides agencies with an irrefutable method of tracing all telecommunications from end-to-end. It can also be used to demonstrate an association between two or more people, prove that two or more people

communicated at a particular time (such as before the commission of an alleged offence), or exclude a person from further inquiry. The attrition of data will have a deleterious impact on law enforcement agencies' intelligence and evidence gathering capabilities. In June 2013 the Parliamentary Joint Committee on Intelligence and Security (PJCIS) concluded that telecommunications industry changes are resulting in 'an actual degradation of the investigative capabilities of the national security agencies, which is likely to accelerate in future'. A European investigation provides an example of the difference data retention can make—in a major Europol child exploitation investigation UK investigators, with the advantage of retained data, identified 240 out of 371 suspects in their jurisdiction (almost 65%) securing 121 convictions; Germany on the other hand, without data retention, identified less than 2% (7 out of 377 suspects) and convicted none.

22. Access to historical data and analysis of inter-linkages with other data sources is vital to both reactive investigations into serious crime and the development of proactive intelligence on organised criminal activity and matters affecting national security. In 2012 the Queensland Crime and Misconduct Commission (now the Crime and Corruption Commission) stated that more than one-fifth of all of their investigations were being undermined by telecommunications data not being kept. In 2014 the Australian Federal Police (AFP) revealed that it could not identify more than one-third of all suspects in a current, major child exploitation investigation, because the telecommunications data is not available.

23. The data retention measures contained in the Bill will ensure the retention of the basic telecommunications data that is essential to support Australian law enforcement and security agencies in the performance of their functions.

24. The Bill will also amend the TIA Act to bolster the privacy protections associated with the access to, and use of, telecommunications data. It will achieve this by limiting the agencies which may authorise access to telecommunications data, and by providing that agencies' access to, and use of, telecommunications data will be subject to comprehensive oversight by the Commonwealth Ombudsman.

25. Notably, the measures contained in the Bill do not increase or otherwise modify the powers of Australian agencies in relation to access to the content of communications.

Parliamentary Joint Committee on Intelligence and Security recommendations on data retention

26. In its Report entitled *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, the PJCIS noted that there was a diversity of views within the Committee as to whether there should be a mandatory data retention regime. The PJCIS observed that whether there should be a mandatory data retention regime was ultimately a decision for Government. However, if the Government was persuaded that a mandatory data retention regime should proceed, provided guidance on the particulars of a data retention regime, including that:

- any mandatory data retention regime should apply only to 'metadata' and exclude content
- the controls on access to communications data remain the same as under the current regime

- internet browsing data should be explicitly excluded
- in the absence of existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years, and
- an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers and oversight of agencies' access to telecommunications data by the Ombudsmen and the Inspector-General of Intelligence and Security (recommendation 42).

27. The proposed data retention scheme is consistent with the majority of the PJCIS's recommendations in relation to any telecommunications data retention obligation.

28. The proposed data retention scheme recognises that the ability to lawfully access telecommunications data held by telecommunications service providers is a vital tool for agencies. Criminals and persons engaged in activities prejudicial to security use the full range of modern telecommunications services to communicate, and coordinate and manage their activities. The availability of encrypted services is also impacting on the utility of access to telecommunications content, making telecommunications data an increasingly valuable investigative tool.

29. The utility of access to telecommunications data is clearly demonstrated in its ability to provide critical evidence and intelligence in terrorist and other criminal prosecutions. There is a risk that if the Government does not imminently address the issue of data attenuation there will be a serious decline in this important investigative capability, and the effectiveness of national security and law enforcement agencies across the nation to prevent or detect serious crime and safeguard national security will be seriously impacted. In addition to being broadly consistent with the PCJIS's views on parameters for a data retention regime, the proposed scheme is reasonable and proportionate to the law enforcement and national security aims to be supported by limiting the retention obligations to categories of data critically required by law enforcement and intelligence agencies to investigate and solve crime and to protect national security. The scheme is also bolstered by refinements to data access arrangements and a new oversight regime, providing important safeguards further contributing towards providing a reasonable and proportional response to the challenges of declining availability of telecommunications data for law enforcement and security purposes.

Overview of Schedules

30. Schedule 1 will require providers of telecommunications services to retain telecommunications data associated with a communication specified in subsection 187A(1) for a period of two years (section 187C). Proposed paragraph 187A(1)(a) provides that the data to be retained is to be prescribed by regulation. The use of regulations to prescribe the details of data to be retained facilitates the prescription of the necessary technical detail to provide clarity to telecommunications service providers about their data retention obligations while remaining sufficiently flexible to adapt to rapid and significant future changes in communications technology. Proposed subsection 187A(2) limits the range of data that may be prescribed to specified categories, providing a limitation on the range of data types the regulations may prescribe for the retention obligation.

31. Proposed subsection 187A(4) will further limit the scope of the regulation making power so that operators of services cannot be required to keep information that is the content or substance of a communication, nor an address to which a communication was sent on the internet from a telecommunications device, or from which a communication was sent on the internet by a telecommunications device, using an internet access service . This limitation expressly provides that the regulation making power cannot be used to require service providers to retain information about subscribers' web browsing history. While the detail of the dataset will be included in the supporting regulations, this Compatibility Statement addresses the data to be retained to the extent that the key attributes of retained data are reflected in this Bill.

32. Schedule 1 will also permit service providers to seek approval of data retention implementation plans, providing industry with the ability to seek endorsement of a strategy to achieve compliance with the data retention obligation over 18 months from the commencement of the obligation. The implementation period will allow industry to achieve compliance over an extended period.

33. The Schedule also permits service providers to seek an exemption from data retention obligations. The exemption framework complements and sits alongside the implementation plan framework, providing further flexibility to ensure data retention obligations may be qualified to the extent appropriate having regard to national security and law enforcement considerations and the objects of the *Telecommunications Act 1997*.

34. Under the exemption framework, the Communications Access Coordinator (the CAC) will be able to exempt service providers from being required to:

- retain telecommunications data at all,
- retain specified telecommunications data in respect of one or more types of telecommunications services,
- retain specified telecommunications data for the full retention period

35. Schedule 1 will provide for the enforcement of the data retention scheme by making the data retention obligation and compliance with any implementation plan subject to civil penalty provisions under the *Telecommunications Act 1997*.

36. Schedule 2 will limit the range of agencies that are able to access telecommunications data and stored communications.

37. The Bill will amend the TIA Act to provide that only criminal law-enforcement agencies are able to access stored communications (and to require the preservation of stored communications). Criminal law-enforcement agencies will be defined to mean:

- interception agencies (Commonwealth, State and Territory police and anti-corruption agencies) that are able to obtain warrants to intercept communications under the TIA Act;
- the Australian Customs and Border Protection Service (Customs); and
- authorities or bodies declared by the Minister as criminal law-enforcement agencies.

38. Proposed subsection 110A(4) will require that in making a determination the Minister have regard to the functions of the body in relation to serious contraventions, the assistance accessing stored communications would have in investigating those contraventions, the extent to which the body is required to comply with relevant privacy frameworks and oversight arrangements.

39. The measures contained in Schedule 2 will similarly reduce the range of agencies that are able to access telecommunications data to 'enforcement agencies', being:

- criminal law-enforcement agencies; and
- authorities or bodies that have been declared by the Minister as enforcement agencies, where the agencies satisfy certain criteria which operational and investigative practices evince a clear and genuine need to access historical telecommunications data for their investigations.

40. Proposed subsection 176A(4) will require that in considering whether to make a declaration, the Minister must have regard to: the functions of the body in relation to the enforcement of the criminal law; administering of a law imposing a pecuniary penalty or relating to the protection of public revenue; the assistance accessing telecommunications data would provide in performing those functions; the extent to which the body is required to comply with relevant privacy frameworks; and oversight arrangements.

41. The limitations on who may access stored communications and telecommunications data are complemented by enhanced oversight through a comprehensive Commonwealth Ombudsman oversight model (Schedule 3).

42. Schedule 3 specifies record-keeping, reporting, oversight and accountability requirements relating to agencies' use of, and access to, telecommunications data. Specifically, the Bill will:

- extend the Commonwealth Ombudsman's remit to facilitate independent oversight of agency compliance with powers exercised under Chapter 3 (stored communications) and Chapter 4 (access to telecommunications data) of the TIA Act, and
- prescribe detailed reporting obligations in relation to access to stored communications and telecommunications data to assess agency compliance with the statutory scheme.

43. Schedule 3 provides support for the Ombudsman oversight role by criminalising circumstances where a person fails to comply with a request to attend before an inspecting officer, to give information or to answer questions from the Ombudsman in relation to compliance by the agency with the provisions relating to access to telecommunications data,

and, in relation to a criminal law enforcement agency, in relation to access to stored communications. The Bill will also create a mirror offence to support the Ombudsman in oversight of the interception of communications. The penalty for these offences is 6 months imprisonment.

Human rights implications

44. The Bill engages the following human rights:

- protection against arbitrary or unlawful interference with privacy contained in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)
- the right to a fair trial, the right to minimum guarantees in criminal proceedings and the presumption of innocence contained in Article 14 of the ICCPR
- protection of the right to freedom of expression contained in Article 19 of the ICCPR, and
- the right to life and the right to security of the person contained in Articles 6 and 9 of the ICCPR (respectively).

Right to protection against arbitrary or unlawful interferences with privacy—Article 17 of the ICCPR

45. The Bill engages the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.

46. The use of the term 'arbitrary' means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' to imply that any limitation must be proportionate and necessary in the circumstances.

47. The right to privacy under Article 17 can be permissibly limited in order to achieve a legitimate objective and where the limitations are lawful and not arbitrary. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted the requirement of 'reasonableness' to imply that any interference with privacy must be proportionate to a legitimate end and be necessary in the circumstances of any given case.

48. In this case, the legitimate end is the protection of national security, public safety, addressing crime, and protecting the rights and freedoms of individuals by requiring the retention of a basic set of communications data required to support relevant investigations.

49. The Bill permissibly limits an individual's privacy in correspondence (telecommunications) in a way which is reasonable and proportionate by circumscribing the types of telecommunications data that are to be retained by service providers to the essential categories of data required to advance criminal and security investigations, permitting access to telecommunications data only in circumstances prescribed by existing provisions in the

TIA Act and moreover reducing the range of agencies who may access data under those provisions.

50. To the extent that the right to privacy is impinged, the interference corresponds to a 'pressing social need', that is, the need for law enforcement agencies to effectively investigate and prosecute crime. The limitation is proportionate because the measures are precisely directed to the legitimate aim being pursued. Rather than requiring retention of a broad range of telecommunications data, the Bill expressly limits the data to be retained to certain types, and moreover excludes data representing a greater level of intrusion.

51. The provisions of the Bill engage the right to privacy in the following manner:

52. Schedule 1: The introduction of a regime whereby service providers must retain a specifically defined set of telecommunications data for a two year period engages the right to privacy. The regime requires that service providers retain and store data, which includes subscriber information, some of which may constitute personal information for the purposes of the *Privacy Act 1998* (the Privacy Act).

53. The Bill also includes a mechanism for the Communications Access Coordinator (the CAC) to exempt a service provider from some or all of the mandatory data retention requirements, with or without conditions or qualifications, either entirely, in respect of a specified kind of service or in relation to the retention period.

54. Schedules 2 and 3: Reduce the number and range of agencies that may access telecommunications data and extending the remit of the Ombudsman to oversight law enforcement agency compliance with the framework for access to, and use of telecommunications data under Chapter 4 of the TIA Act. Schedules 2 and 3 also extend and enhance the Ombudsman's oversight of law enforcement agencies' access to, and use of, stored communications. These amendments promote protection from unlawful and arbitrary interference with privacy by ensuring that access to data only occurs in confined circumstances as dictated by operational need and that the ability to become an agency who may access telecommunications data is closely circumscribed and subject to parliamentary disallowance. Protection from unlawful and arbitrary interference is likewise promoted by the conferral of an oversight role on the Ombudsman. The prospect of review and accountability provides a strong and positive incentive for strict compliance, thereby supporting privacy protection and obviating against unlawful or arbitrary interference with this right.

Schedule 1—Data retention obligations and mandatory dataset

55. Schedule 1 will amend the TIA Act to create a requirement for service providers to retain certain types of telecommunications data prescribed by regulation for two years. The framework allows service providers to seek exemptions for the requirement from the Communications Access Co-ordinator, supporting providers to not retain data in respect of telecommunications services that may be of lesser relevance to law and security purposes. The ability to grant exemptions provides a further mechanism to minimise privacy intrusion through the retention of telecommunications data having regard to the interests of law enforcement and national security.

56. Proposed section 187A of the Bill requires that service providers retain prescribed information or documents in relation to the use of their services. Proposed

subsection 187A(2) limits the types of information that may be prescribed to information relating to subscribers to a service, the characteristics of an account or device relating to a service, the source, destination and timing of a communication, the type of communication and the location of a device used in connection with a communication. Details of the data falling within these circumscribed classes will be contained in regulations.

57. The legislative requirement for providers to store the telecommunications data in relation to its services engages the right to protection against arbitrary and unlawful interference with privacy. The specification of the types of data that may be prescribed serves to minimise the privacy impacts associated with the storage of telecommunications data, ensuring that only narrow categories of telecommunications data necessary for the investigation of serious criminal offences and national security threats are retained. In summary, privacy and other rights-based implications are minimised because:

(1) the data that may be prescribed for retention is confined in ambit so that only non-content data which is critical to initiating or furthering law enforcement investigations is required to be retained;

(2) the data retention regime is supported by new Commonwealth Ombudsman oversight of agency access to and use of telecommunication data, coupled with existing statutory obligations under the Privacy Act in relation to privacy protections and accountability standards for service providers in relation to customers' personal information, consistent with contemporary community expectations; and

(3) the scheme will be reviewed three years after the conclusion of the implementation phase of the obligation, providing an opportunity for further Parliamentary scrutiny of the proportionality and effectiveness of the response and impact on privacy.

Security and destruction of retained data

58. The Bill contains a range of safeguards to ensure that the rights of individuals, in particular the privacy rights of individual telecommunications users, are protected. The right to privacy is permissibly limited and the limitation is reasonable, necessary and proportionate to a legitimate aim.

59. Telecommunications service providers currently retain, store and destroy a wide range of telecommunications data for their own purposes and to comply with other legislative obligations. Accordingly, service providers already have arrangements for the storage and protection of this information consistent with their existing data protection obligations under the Privacy Act or state/territory equivalent legislation. The Australian Privacy Principles (APPs) in the Privacy Act apply to personal information held by regulated entities, including service providers that will be required to retain data in accordance with the provisions of the Bill.

60. Telecommunications data covered by the retention scheme may, in some circumstances, constitute personal information and, as such be subject to the protections set out in the APPs. The Privacy Act and proposed Telecommunications Sector Security Reforms (TSSR)[1] will, in combination, require service providers to do their best to prevent

[1] The Privacy Act sets out the circumstances in which a carrier or carriage service provider (C/CSP) may use or disclose personal information, and sets out detailed requirements that must be met before a C/CSP may disclose

unauthorised access to and unauthorised interference with retained telecommunications data. In addition, the Privacy Commissioner will continue to have oversight of carriers' collection and retention of personal information under the Bill where service providers are subject to the Privacy Act, including the ability to conduct assessments to ensure compliance with the APPs.

61. The privacy implications associated with the increased volume of data which may be generated by the mandatory dataset arrangements are mitigated by the existing statutory obligations on service providers to ensure the quality and/or correctness of any personal information (APP 10) and to keep personal information secure (APP 11) as well as in relation to destruction of personal information. Telecommunications service providers currently retain information of the type which is being contemplated under the data retention scheme for their own functions and purposes, including billing customers.

62. To the extent that some service providers may not be required to comply with the APPs, retained data would be subject to the same security standards as other data on a service providers' network. This would include the application of technical and organisational measures to ensure the confidentiality, integrity, and availability of the retained data to ensure that the retained data can only be accessed by authorised personnel.

63. Further, service providers which are non-APP entities are subject to the data protection obligations contained in Part 13 of the Telecommunications Act. Under section 309 of the Telecommunications Act, the Information Commissioner oversees compliance by telecommunications providers with Part 13 of that Act. This includes monitoring the record-keeping of service providers and ensuring that the grounds for disclosures under Part 13 are recorded by service providers and authorised by the Telecommunications Act and the TIA Act.

The prescribed dataset

64. Proposed section 187A sets out the types of information and documents that service providers may be required to retain in accordance with the proposed mandatory data retention obligation. While the detail of the dataset will be provided in supporting regulations, this Compatibility Statement examines rights engaged by a mandatory data regime having regard to the type of data which it is envisaged would form part of the data set enumerated in proposed section 187A.

65. *Paragraph 187A(2)(a)—subscriber of the relevant service and accounts, telecommunications devices and other relevant services relating to the relevant service:* Information regarding the subscriber of a relevant service is information that is critical for linking the identity of a person to the use of a relevant service. Information about accounts, telecommunications devices and other relevant services relating to the relevant service likewise provide basic and essential information about the subscription to and use of a relevant service.

---

personal information outside Australia. The proposed Telecommunications Sector Security Reform, as recommended by the Parliamentary Joint Committee on Intelligence and Security, will involve introducing a new obligation on C/CSPs to do their best to prevent unauthorised access and unauthorised interference to telecommunications networks and facilities, including where a C/CSP outsources functions.

66. The information covered by paragraph 187(2)(a) is essential for any investigation involving communications made from a service, as it enables investigating authorities to establish the details of who is involved in making a communication. This type of information is already broadly retained by service providers as part of general customer records for up to 7 years.

67. The retention of this data category is reasonable, proportionate and necessary in fulfilment of the legitimate aim of ensuring law enforcement and intelligence agencies have the investigative tools to safeguard national security and prevent or detect serious and organised crime. In the absence of the retention of this type of information, it may be exceedingly difficult or impossible to determine who has made a communication of interest. Subscriber information provides the critical link between communications and the subscriber to the service. Without this basic information, agencies may be unable to commence an investigation, as it can otherwise be impossible to link a suspect communication to a particular subscriber, thereby providing no avenues to further investigations. This is particularly the case in relation to crime types making extensive use of telecommunications in their perpetration, for example the distribution of child pornography. It is notable that subscriber data, as the predominant data category which would be generated through the collection of customer information, raises relatively fewer privacy implications than traffic and location data comparators.

68. *Paragraph 187A(2)(b)—the source of a communication*: This category covers the identifier or combination of identifiers which are used by the service provider to describe the account, service and/or device from which a successful or attempted communication is sent. An example of such an identifier is a telephone number. The source of a communication is critical for the purpose of the investigation, detection and prosecution of serious crime and security threats, providing clear identification of the origin of communications relevant to investigations.

69. *Paragraph 187A(2)(c)—the destination of a communication*: This category covers identifiers of an account to which a communication is sent. An example of such an identifier is the telephone number dialled when making a telephone call. The retention of telecommunications data regarding the destination of a communication (such as telephone numbers and email addresses) is necessary in order to connect a communication of interest to the particular telecommunications service being used to send or receive this communication. This information can then assist with determining the subscribers who sent or received relevant communications. If providers of telecommunications services did not retain this telecommunications information, there is a real risk that agencies would not be able to determine with whom a person has been communicating, providing important information on linkages and connections of investigative significance and which are critical to advance inquiries into criminality and security threats.

70. Under proposed paragraph 187A(4)(b), the retention obligation is explicitly expressed to exclude the retention of destination web address identifiers, such as destination internet Protocol (IP) addresses or uniform resource locators (URLs). This exception is intended to ensure that providers of internet access services are not required to engage in session logging, which may otherwise fall within the scope of the destination of a communication.

71. *Paragraph 187A(2)(d)—the date, time and duration of a communication*: This category covers the time at which it occurred and its duration. Using this information,

agencies can link the time of a communication with events associated with the communication. This information is also critical to linking a communication to a particular subscriber, as the source of a communication can change over time, requiring the time of the communication in order to identify its sender.

72. The retention of this data category is reasonable, proportionate and necessary as it constitutes information that can help inculpate or exculpate an individual associated with a communication, and is also valuable in tracing the steps of a missing person who has been using a communications service before or during the time they are missing. An agency's ability to investigate these matters will be significantly limited if providers of telecommunications services do not retain this information. The data covered by this item is also critical because communications may now travel over multiple networks and service providers. As such, time-calibrated information about a communication needs to be sufficiently precise to enable agencies to develop an accurate picture of a particular communication.

73. *Paragraph 187A(2)(e)—the type of communication*: This category covers the type of service used, including the type of access network or service or application service. Data which identifies the type of communication is necessary for understanding what telecommunications service has been used to send the communication.

74. *Paragraph 187A(2)(f)—the location of the line, equipment or telecommunications device*: This category covers information which identifies equipment used in connection with a communication.

75. Information on the location of telecommunications equipment can be of significant utility to law enforcement and national security investigations. Location information is often retained in records which form a part of a customer's billing.

76. The potential privacy impacts associated with the retention of information which determines the location of equipment has been minimised in the Bill. The Bill provides that two or more communications that together constitute a single communications session, such as an internet access session, are taken to constitute a single communications session. This limitation ensures that communications that may technically be achieved by a series of smaller communications, such as a download, are treated as a single communication, and through that ensuring that location information is limited to that overarching communication rather than its constituent components. Further, the Bill expressly provides that the obligation to keep location information is limited to location information used by the service provider to provide the relevant service. Accordingly, the obligation is limited to that required by the networks to effect a communication, but cannot extent to other location based information that a provider may hold.

77. Location-based data is valuable for identifying the location of a device at the time of a communication, providing both evidence linking the presence of a device to an event, or alternative providing indications that may exclude a person from further inquiry. This data may also be instructive in determining the location of a person who is reporting an emergency, or help with precursory steps towards identifying the locality of a missing person who has used a telecommunications device. Without this information being retained by service providers, agencies' abilities to investigate crimes, emergencies and missing person matters are substantially limited.

78. While service providers typically generate a wide range telecommunications data in the course of providing telecommunications services, the Bill further circumscribes the data retention obligation by excluding information that the service provider is required to delete pursuant to a Determination made under section 99 of the Telecommunications Act. This ensures that the limitation on the privacy of users of telecommunications services is proportionate to the legitimate outcome sought, that being the ability for Australian law enforcement and national security agencies to have the necessary telecommunications data to effectively carry out their investigations, and does not operate to require retention of a specific category of subscriber identification information required to be destroyed under specific existing protections.

79. Importantly, access to all telecommunications data (whether or not captured by the terms of the data set) is strictly reserved for specific purposes under the TIA Act. Enforcement agencies may only issue authorisations enabling access to data where it is 'reasonably necessary' for a legitimate investigation and must consider the privacy impact of accessing telecommunications data. 'Reasonably necessary' is not a low threshold. It will not be 'reasonably necessary' to access data if it is merely helpful or expedient. In relation to the Australian Security Intelligence Organisation (ASIO), ASIO is subject to strict privacy and proportionality obligations under the Attorney-General's Guidelines, made under paragraph 8(1)(a) of the *Australian Security Intelligence Organisation Act 1979*, which relevantly requires that:

- any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence,
- inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions, and
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

80. Notably, the limited telecommunications data the subject of the proposed data retention obligation is information about a communication—not the content or substance of a communication, such as the body and subject line of an email or what you search for online. Agencies will continue to require a warrant to access the content of a communication.

EU Data Retention Directive[2]

81. In the recent judgment of the Court of Justice of the European Union (CJEU) *(Digital Rights Ireland Ltd and Ors (C-293/12) and Kärntner Landesregierung and Ors* (C-594/12), 8 April 2014) the CJEU observed that legislation on the retention of telecommunications data 'must lay down clear and precise rules governing the scope and application' of the measures in question, 'imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against risk of abuse and against any unlawful access and use of that data' (at paragraphs 65-69).

[2] *Judicial consideration of Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* [2006] O J L 105/54.

82. The CJEU accepted that the objective of the EU Data Retention Directive, namely to contribute to the fight against terrorism and serious crime and to maintain public security, was a legitimate justification for interfering with the right to privacy. However, the CJEU considered that the extent of interference as set out in the Directive was disproportionate to those ends.

83. The CJEU considered that the conditions under which data could be retained should have been more closely defined in the Directive, and identified a range of conditions and safeguards which were not included in the Directive and which it considered should have been for human rights compatibility. In particular, the CJEU found that the Directive was not human rights compatible because it did not contain:

a. any restrictions on the types of data retained—the Directive covered all persons, all means of electronic communications and all traffic data (paragraph 57)

b. any conditions limiting the categories of data that is retained—for example limitations by geographical location, or by link to serious crime (paragraph 59)

c. any objective criteria on access to data and its subsequent use, simply referring to 'serious crime' and did not restrict access to the purpose of preventing/detecting serious crime (paragraph 60)

d. any requirement of prior review by a court or independent administrative body to determine the necessity of the request for the purposes of preventing or detecting serious crime (paragraph 62)

e. any different retention periods for different types of traffic data, or any requirement that the retention period be based on objective criteria (paragraph 57), and

f. sufficient safeguards for the protection of data, having regard to the quantity of data retained, the sensitive nature of the data, and the risk of unlawful access to the data (paragraph 66).

84. In relation to the scheme proposed in the Bill, the types of information that may be prescribed for retention are consistent with those identified in the Directive, but the proposed scheme provides a mechanism to provide clear and specific restrictions on the nature of the data to be retained by regulation (criteria (a)). The dataset does not apply indiscriminately to all details of electronic communications to the extent that it does not require retention of all traffic data in its various permutations. In addition, the proposed obligation is explicitly expressed to exclude web-browsing history and to limit location information to that held by a carrier in connection with the provision of the service.

85. In relation to criteria (c) and (f), Schedules 2 and 3 introduce provisions to reduce the number of agencies who may access telecommunications data and implement new and comprehensive oversight of access to, and usage of, this data. This will be achieved by: amendments to the definition of 'enforcement agency' in section 5 of the TIA Act to confine its ambit; replacing the existing general descriptors of the types of agencies who may access telecommunications data with a confined list, combined with a ministerial declaration scheme to ensure that any additions to the range of agencies is rigorously assessed against

their functions, need for access to data, privacy protections and oversight arrangements; and providing independent oversight for agency access telecommunications data by extending the statutory remit of the Commonwealth Ombudsman to enable the Ombudsman to oversight agency use of, and access to, telecommunication data.

86. These new measures to countermand the risk of unlawful access to telecommunications data are also supported by continued application of existing privacy protection frameworks. In relation to criteria (d) the reduction in the number of agencies capable of accessing data and the introduction of a ministerial declaration scheme will ensure scrutiny of any extension to the agencies that may access telecommunications data. In relation to criteria (e), the measure caps the mandatory retention period of retention at two years. The retention period is based on objective determinants associated with the descriptive nature and confined classification of the data types which form the dataset. The retention period reflects international experience that, while the majority of requests for access to telecommunications data are for data that is less than 6 months old, certain types of investigations are characterised by a requirement to access to data up to 2 years old. These include complex investigations such as terrorism, financial crimes and organised criminal activity, serious sexual assaults, premeditated offences and transnational investigations. Against the particular context of the critical importance of telecommunications data in very serious crime types and security threats, the two year retention period provides a proportionate response to that environment.

CAC exemption regime

87. Proposed Division 3, Part 5-1A of the TIA Act provides for a mechanism for the CAC to grant an exemption to a service provider from some or all of the mandatory data retention obligations. The scheme will operate in a similar way to the existing exemption regime for interception capability provided for under section 192 of the TIA Act.

88. Under the data retention exemption scheme, a service provider may apply to the CAC for an exemption and the CAC would be required to make a decision on the application within a specified period. The exemption may also stipulate expiration dates or circumstances whereby the service provider must reapply for an exemption.

89. The CAC exemption facility indirectly strengthens the right to privacy of individual customers in that it provides a method of reducing data retention obligations, for example, in circumstances where the volume of data to be retained is disproportionate to the interests of law enforcement and national security.

Review of data retention scheme

90. A further important public accountability and transparency measure contained in the Bill is proposed section 187N which provides for a review of the data retention regime three years after the conclusion of the implementation phase. This responds to the PJCIS recommendation that ‘the effectiveness of the regime be reviewed by the PJCIS three years after its commencement.’ The data retention scheme will not be fully functional until at least two years after its commencement as industry begins to collect and retain the required data in accordance with the implementation arrangements. In addition, investigations and prosecutions span many years, and they provide the most effective barometer through which the data retention scheme is best empirically assessed. Review three years after the

conclusion of the implementation phase will provide both practical industry experience and a sound evidence base for considering the operation of the scheme.

Two year retention period

91. Proposed section 187C will provide that the data retention period for all classes of data subject to the scheme will be two years.

92. Law enforcement and national security agencies advise that a data retention period of two years is appropriate to support critical investigative capabilities. The proposed two year period draws on international experience in relation to the use and value of telecommunications data and achieves a balance between supporting the operational requirements of agencies and minimising privacy impacts associated with the retention of data. Experience under the former EU Data Retention Directive was that, while frequently data accessed by agencies was less than six months old, there was a higher requirement for data up to two years old for national security and complex criminal offences.

93. Data retention beyond the statutory retention period will continue to be governed by industry business needs, other legislated requirements (such as those relating to tax records), privacy protection obligations under Part 13 of the Telecommunications Act or the Privacy Act. The Bill will not prevent a provider from keeping records for these purposes.

Schedule 2—Agency use of preservation notices, access to stored communications and access to telecommunications data

94. Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an 'enforcement agency' to authorise a carrier to disclose telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. Lawful access to the telecommunications data is subject to existing safeguards contained in the TIA Act. The TIA Act establishes a process of authorisation for access to telecommunications data that requires senior management officers of agencies to authorise access to this data before it is disclosed to the agency. The authorisation process requires the authorised officer to consider the need for access to this information on a case-by-case basis in accordance with a prescriptive legal framework. There are separate provisions enabling access by ASIO for purposes relevant to security.

95. Currently, under the TIA Act, an enforcement agency is broadly defined as all agencies empowered to intercept telecommunications content as well as bodies whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. The range of agencies that are enforcement agencies and which are capable of authorising the disclosure of telecommunications data is broad and includes Commonwealth, State, Territory and local government agencies as well as non-government or quasi-government bodies that carry out relevant functions.

96. The Bill will amend the definition of 'enforcement agency' to clearly circumscribe the agencies who may access telecommunications data, ensuring that access is limited to those agencies who have a clear and scrutinised need for access to telecommunications data in the performance of their functions and are subject to appropriate privacy and oversight arrangements.

97. Schedule 2 of the Bill engages the right to privacy under Article 17 of the ICCPR on the basis that the telecommunications data retained pursuant to subsection 187A(1) will be accessible by agencies in accordance with the existing lawful access provisions permitted under the TIA Act. The Bill does not lower the statutory threshold under which agencies are able to access telecommunications data. Rather, the TIA Act ensures telecommunications data is only accessible through existing processes for lawfully accessing telecommunications data.

98. In order to reinforce the privacy protections associated with a user's telecommunications data contained within the TIA Act, Schedule 2 of the Bill introduces limitations upon the type of agencies that are permitted to authorise the disclosure of telecommunications data for an agency's investigations. The Bill also places new limitations on the range of agencies that can access stored communications such as emails and SMSs, by further confining the scope of agencies that can apply for stored communications warrants and issue preservation notices under Chapter 3 of the TIA Act.

99. The proposed refinements to the definition of enforcement agency, coupled with the ministerial declaration models which would govern access, are will ensure that data access arrangements are rigorously scrutinised. Consistent with the nature of the powers that are reposed in enforcement agencies under Chapter 4 and their impact on privacy, the definition of an enforcement agency appropriately circumscribes the access regime and introduces explicit ministerial and parliamentary scrutiny.

100. The factors the Minister must consider when determining whether to declare an authority or body to be a *criminal law-enforcement agency* or an *enforcement agency* will include:

- whether the authority or body undertakes investigative or public protection responsibilities which would necessitate access to stored communications and telecommunications data respectively,
- whether the authority or body has processes and procedures in place that would satisfy the Minister that the information, if accessed, would be used in a manner which seeks to minimise the privacy impacts on any persons to whom the data relates or is appreciably linked to, and
- whether the Minister considers that the declaration would be in the public interest.

101. The public interest criteria ensures that the Minister gives consideration to matters of community expectation, which would include, but not be limited to, the proper administration of government; public health and safety; national security; and the prevention and detection of crime and fraud.

102. The Bill provides that a key factor in considering whether to declare an agency to be an enforcement agency includes the extent to which the agency is required to comply with the Australian Privacy Principles or a similar protective arrangement. Where an authority or body is a non-APP entity, then the Minister must consider the agency's compliance with a binding scheme that provides a comparable level of protection to personal information (for example, under equivalent State or Territory equivalent privacy legislation) or other arrangements to provide similar or equivalent levels of protection to personal information when handling any personal information disclosed to it by a carrier under Chapters 3 and 4 of the TIA Act.

103. The Bill will explicitly enable the Minister to revoke a declaration where the Minister is no longer satisfied that the circumstances justify the authority or body having access to telecommunications data.

104. The ministerial declaration scheme reinforces the right to privacy in that it ensures that enforcement agency access to telecommunication data is strictly circumscribed and subject to ministerial scrutiny. This provides a critical safeguard and restricts such access to agencies which have satisfied the Minister that they have a genuine and demonstrated need for access to telecommunications data. The Minister may, of his or her own motion, revoke a declaration if he or she is no longer satisfied that the circumstances continue to justify access to telecommunications data. Importantly, the declaration process allows the Minister to impose conditions on access, which provides a further ability to restrict and confine access to telecommunications data in a manner consistent with and proportionate to the needs of the agency to be declared in all the circumstances.

105. The Bill also amends Chapter 3 of the TIA Act to confine and limit those agencies that are able to apply for stored communications warrants and issue preservation notices. While the TIA Act currently provides that *enforcement agencies* are able to apply for these stored communications warrants and issue preservation notices, the Bill will repeal these provisions and amend the TIA Act to provide that only *criminal law-enforcement agencies* are able to utilise these investigative powers.

106. *Criminal law-enforcement agencies* are defined in the Bill to include Australian police forces and anti-corruption agencies that currently have the ability to apply for warrants for the interception of telecommunications. The Bill provides that the Minister may declare additional agencies to be *a criminal law-enforcement agency* subject to consideration of specified criteria prescribed in the Bill. As a corollary of the higher level of intrusion into privacy occasioned by access to stored communications and prospective telecommunications data, a higher threshold for an agency to be declared as a *criminal law-enforcement agency* applies in comparison to the criteria applicable for *enforcement agency* status. Like the declarations for *enforcement agencies*, agencies must similarly demonstrate that access to stored communications information is necessary for their investigative functions.

107. The Bill will not lower the threshold of access to stored communications in Chapter 3, but substantially reduces the number of agencies who may seek to access stored communications by redefining the concept of a criminal law enforcement agency in the TIA Act.

108. Collectively, the proposed amendments in relation to the range of agencies that may access stored telecommunications or telecommunications data contribute to ensuring that access is reasonable, necessary and proportionate. The existing frameworks in relation to access to, use and disclosure of this lawfully accessed information in the TIA Act will continue to ensure that any abrogation on the privacy right in Article 17 is limited to the legitimate purposes articulated in the TIA Act.

Schedule 3—Oversight and accountability provisions

109. Schedule 3 will extend the remit of the Ombudsman to enable the Ombudsman to comprehensively assess agency compliance with all of an enforcement agency's (or a criminal law-enforcement agency's) obligations under Chapters 3 and 4 of the TIA Act, including use and access to telecommunications data. Oversight of this category of data

would also extend to auditing the use and access to data retained as a result of the data retention obligation.

110. There is currently no independent oversight for the use of, and access to, telecommunications data. Neither the TIA Act nor the predecessor arrangements in the Telecommunications Act included an independent oversight arrangement in relation to telecommunications data. The Bill will facilitate Ombudsman oversight of access to and use of telecommunications data.

111. The oversight arrangements draw on the model contained in Part 6 of the *Surveillance Devices Act 2004* (Cth) (the SD Act) and aspects of the oversight role performed by the Commonwealth Ombudsman under Part IAB of the *Crimes Act 1914* (Cth). The oversight model extends beyond agency record keeping and record destruction of obligations and provides a higher level of guidance in terms of the precise obligations imposed on law enforcement agencies. The model therefore supports compliance by agencies due to the higher level of precision in compliance obligations, greater consistency in reporting methodology by agencies and higher acuity in statistical output to measure compliance for annual reporting and other audit-related purposes.

112. Schedule 3 will vest the Ombudsman with an over-arching role in assessing agency compliance across powers exercised under both Chapters 3 (stored communications) and 4 (telecommunications data) of the TIA Act. Currently under the TIA Act, the Commonwealth Ombudsman's audit functions in relation to stored communications are limited to compliance with an agency's record keeping and record destruction obligations. The Bill will expand the Ombudsman's oversight role in a manner consistent with that proposed for oversight of access to telecommunications data.

113. Currently, the emphasis of the Ombudsman's oversight role under Chapters 3 of the TIA Act is on determining agency compliance with record keeping and destruction provisions. The enhanced oversight function proposed under Chapter 4A of the Bill will enable assessment of an enforcement agency's overall compliance with the powers exercisable under Chapters 3 and 4 of the TIA. The proposed provisions relating to the powers, scope and reporting obligations of the oversight role would enable the Ombudsman to provide a level of public accountability as to how agencies have applied their powers under Chapters 3 and 4.

114. The proposed oversight model promotes Convention rights, by virtue of the following key features:

- holistic oversight of enforcement agency use of and access to telecommunications data (beyond agency record keeping and record destruction of obligations) to ascertaining agencies' compliance in exercising their powers under Chapter 3 and Chapter 4 of the TIA Act (excluding ASIO, which is the subject of separate independent oversight)
- a higher level of specificity and transparency in terms of the precise reporting obligations imposed on law enforcement agencies
- consistency in inspection methodology by virtue of a non-fragmentary model involving oversight of all agencies that apply the powers under Chapters 3 and 4, and
- clearly defined reporting obligations that will engender:

- a higher level of compliance by agencies due to a greater level of precision in compliance obligations, and

- greater acuity in statistical output to measure compliance for annual reporting and cross-agency compliance.

115. The Bill promotes the right to privacy by confirming the Ombudsman's ability to audit an agency's use of its powers to access stored communications and telecommunications data under the TIA Act. This helps ensure that an agency's access to the telecommunications information of interest to an investigation, and the interaction with the privacy right in Article 17 in that regard, is a reasonable, necessary and proportionate limitation on that right to privacy.

116. These measures are consistent in-principle with the PJCIS's recommendation that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the TIA Act.

117. The proposed Ombudsman oversight of the telecommunications data regime recognises that access to telecommunications data by enforcement agencies potentially impacts on the privacy of persons whose data is being accessed. It is responsive to privacy and other rights-based issues raised by the implementation of the new data retention regime and the ability for enforcement agencies to access telecommunications data. A comprehensive oversight regime for telecommunications data will assist in ensuring that use, access or disclose telecommunications data by enforcement agencies, including retained data, for purposes set out in Chapter 4 of the TIA Act, is subject to independent compliance assessment. It will also serve to provide an important level of public accountability and scrutiny of agency practices by virtue of the Ombudsman public reporting regime proposed to be implemented in Chapter 4A.

Right to a fair trial

118. The Bill engages Article 14 of the ICCPR, which guarantees a person be afforded a fair hearing in relation to any suit at law and in the determination of any criminal charge against them, the right to a fair trial in the following respects:

- the imposition of civil penalty provisions in relation to a failure to comply with subsections 187A(1) and 187D(a) (subsection 187M),
- the imposition of criminal offence provisions contained in proposed subsections 87(6) and 186C(3), and
- the privilege against self-incrimination engaged by subsection 186D(1) and (2).

Proposed section 187M

119. Proposed section 187M will provide that civil penalties may apply where a service provider fails to keep or cause to be kept information or documents as required by the data retention obligation or where a service provider fails to comply with an approved data retention implementation plan in respect of a communication carried by means of that service.

120. The effect of this provision is that contraventions of statutory obligations in relation to the data retention regime are dealt with under the enforcement mechanisms specified under the Telecommunications Act. Enforcement options available under the Telecommunications Act include remedial directions, formal warnings, pecuniary penalties and infringement notices.

121. The United Nations Human Rights Committee has stated that the notion of criminal charges may 'also extend to acts that are criminal in nature with sanctions that, regardless of their qualification in domestic law, must be regarded as penal because of their purpose, character or severity' (see General Comment No. 32, para 15; Communication No. 1015/2001, *Perterer v Austria*, at para 9.2). As such, a penalty or other sanction, notwithstanding its nomenclature, may be 'criminal' for the purposes of the ICCPR even if it is described as a civil penalty under Australian domestic law. It is therefore necessary to consider the substance as well as the form of the civil penalties provided for by the Bill.

122. The civil penalty in proposed subsection 187M is not, in substance, a criminal penalty provision. Rather, the provision forms part of a regulatory regime which provides for a graduated series of sanctions under the Telecommunications Act, including infringement notices and pecuniary penalties. It is aimed at an objective which is protective or regulatory (the critical objective being to ensure provider compliance with the obligations imposed by the Bill) as opposed to being punitive or reparatory in nature.

123. The civil penalty provision is designed to ensure a proportionate regulatory response to redress systemic compliance issues as opposed to acts of moral culpability. Further, no term of imprisonment is provided (typical of a criminal penalty provision) and the maximum penalty is comparatively lower than would be imposed under counterpart criminal penalty provisions. Although it may be regarded as large, it is not excessive in that it applies to regulated enforcement agencies and is reasonable and proportionate having regard to the legitimate community interest in enforcing the obligation to retain selected telecommunications data to support its availability to law enforcement and security agencies.

124. As the penalty provisions which apply in relation to subsection 187A(1) and paragraph 187D(a) are properly characterised as civil penalty provisions, the criminal process guarantees in Article 14 and 15 do not apply. However, the equality of arms principles in Article 14(1) is enlivened because this principle applies equally to civil proceedings. 'Equality of arms' requires that each party be afforded a reasonable opportunity to present its case under the conditions that do not place it at a substantial disadvantage vis-à-vis another party (*Brandstetter v. Austria*, Application No: 11170/84; 12876/87; 13468/87, Strasbourg judgment 28 August 1991 §§41-69)). 'Equality of arms' essentially denotes equal procedural ability to state the case. The right of equal access to a court, embodied in Article 14(1), is engaged, but not limited by proposed section 187M. This is because the imposition of a civil penalty in these circumstances does not derogate from, or abridge, existing procedural rights of parties to litigation and would not result in actual disadvantage or other unfairness to the defendant. That is, the provision would not impact upon opportunities to adduce or challenge evidence or present arguments on the matters at issue (*H. v Belgium*, Application No: 8950/80, Strasbourg judgment 30 November 1987 §§49-55). Further, the provision in no way impedes parties to a relevant proceeding being given the opportunity to contest all the arguments and evidence adduced.

Criminal penalty provisions—subsection 186C(3) and subsection 87(6)

125. Proposed subsection 186C(3) will make it a criminal offence to refuse to attend before an inspecting officer, to give information or to answer questions where requested by an inspecting officer of the Ombudsman for the purposes of inspections conducted under new Chapter 4A. The maximum penalty for this offence is 6 months imprisonment.

126. Proposed subsection 87(6) will similarly make it a criminal offence for a person to fail to comply with a request to attend to provide information, to give information or to answer questions from the Ombudsman under section 87 where the Ombudsman has reason to believe that an officer of an agency is able to give information relevant to an inspection under Chapter 2, Part 2-7 of the TIA Act. The maximum penalty for this offence is 6 months imprisonment.

127. Both offence provisions mirror existing provisions in the SD Act (section 56) and *Inspector-General of Intelligence and Security Act 1986* (section 18).

128. Criminal penalty provisions of this nature engage the criminal process rights under Article 14 of the ICCPR. This Article sets out specific guarantees that apply to proceedings involving the determination of 'criminal charge', and to persons who have been convicted of a 'criminal offence'.

129. The proposed offence provisions are reasonable and proportionate and do not impermissibly limit the criminal process guarantees under the ICCPR. To the extent they engage Article 14, they are unlikely to raise any issues of incompatibility with Article 14(2) of ICCPR as they involve low penalties and relate to matters that are readily accessible and peculiarly within the defendant's knowledge. It is reasonable to expect law enforcement officers who access regulated powers to comply with conditions associated with inspection and auditing of the exercise of those powers and to respond to relevant requests for information.[3]

130. The proposed offence provisions moreover apply only to people who opt-in to the regulatory regime—people are not compelled to become law enforcement officials, and officials are not compelled to work in investigations and use the powers and therefore potentially be exposed to penalties of this nature. The enforcement agency officers to whom the offences would apply are best placed to make out a valid defence.[4] The facts pertaining to any alleged infringement are readily provable by a law enforcement officer as a matter peculiarly within their own knowledge or to which they have ready access.[5] That is, they are capable of effective rebuttal by an officer of the agency who would be subject to the offence provisions.[6]

131. It is notable that the proposed offence provisions would apply only to officials of law enforcement agencies. Such officials hold positions of great public trust and exercise covert powers under the TIA Act. Public confidence in the justice system requires that officials are

[3] *R v Wholesale Travel Group Inc* [1991] 3 SCR 154.
[4] Attorney-General's Reference (No 4 of 2002) [2005] 1 AC 264; see also *R v DPP; ex parte Kebilene* [2000] 2 AC 326.
[5] *R v Johnstone* [2003] UKHL 28.
[6] *Pham Hoang v France* (1993) 16 EHRR 53.

held to a higher standard of conduct, particularly because there are fewer avenues to identify misconduct in relation to powers exercised covertly.

Proposed subsections 186D(1) and (2)

132. Article 14(3)(g) of the ICCPR protects the right to be free from self-incrimination by providing that a person may not be compelled to testify against him or herself or to confess guilt. The right to be free from self-incrimination may be subject to permissible limitations, provided that the limitations are for a legitimate objective, and are reasonable, necessary and proportionate to that objective.

133. International jurisprudence suggests that the abrogation of the privilege against self-incrimination is more likely to be permissible where protections relating to the use of the information are included, such as a 'use immunity', which prohibits use of the information against the person in subsequent proceedings; or a 'derivative use immunity', which additionally prevents other information obtained as a result of the giving of self-incriminating information being used as evidence against the person.

134. Proposed subsection 186D(1) abrogates the privilege against self-incrimination as it provides that a person is not excused from giving information under new Chapter 4A by reason that compliance would be incriminating. However, provision is made in subsection 186D(2) for use and derivative use immunities that restrict any direct or indirect use of that information in any subsequent criminal or civil proceedings, except by way of a prosecution for an offence against sections 133, 181A, 181B or 182, or against Part 7.4 or 7.7 of the Criminal Code.

Proposed subsection 186D(1)

135. Proposed subsection 186D(1) will provide that a person is not excused from giving information, answering a question or giving access to a document (disclosing information), as required under Chapter 4A (oversight by the Commonwealth Ombudsman) of the TIA Act, despite other matters which may otherwise bar the giving of that information. These matters are listed at proposed paragraphs 186D(1)(a) to (c) and are that disclosure of the information would be:

a. a contravention of a law

b. contrary to the public interest, or

c. might tend to incriminate the person or make the person liable to a penalty.

Privilege against self-incrimination or self-exposure to a civil penalty

136. Proposed paragraph 186D(1)(c) will abrogate the privilege against self-incrimination or self-exposure to a civil penalty (referred to hereafter together as 'self-incrimination') in relation to the disclosure of information required under Chapter 4A. Proposed subsection 186D(2) will however provide that the disclosed information cannot be used as evidence against the person who disclosed that information, whether directly or indirectly (a 'use immunity' and 'derivative use' immunity). The use and derivative use immunities do not apply to prosecutions for offences against sections 133, 181A, 181B and 182 of the TIA Act or Part 7.4 or 7.7 of the Criminal Code.

137. Section 133 of the TIA Act creates an offence of unlawful dealing in accessed stored communications under Chapter 3, Part 3-4, Division 1 of the TIA Act. Sections 181A, 181 and 182 create offences for unlawful dealing in telecommunications data authorisation information or unlawful secondary disclosure of accessed telecommunications data under Chapter 4, Part 4-1, Division 6 of the TIA Act. Parts 7.4 (false or misleading statements) and Part 7.7 (forgery and related offences) of the Criminal Code create offences relating to hindering, obstructing, intimidating or resisting a public official in the performance of their functions.

138. The abrogation of the privilege in relation to the specified offences is reasonable and proportionate in the circumstances for the following reasons:

- there are no other appropriate avenues for collecting this information, which is peculiarly within a person's knowledge and not contained elsewhere in written documentation form (for example, the motive of a person in acting in a particular way); or
- the public benefit derived from the abrogation of the privilege decisively outweighs the harm to individual rights. The harm to individual rights is minimised by the provision of a use and derivative use immunity. The limitation of the immunity to exclude listed offences corresponds with the likely focus of an Ombudsman investigation under new Chapter 4A, and it would frustrate the purpose of Ombudsman oversight if it were not possible for prosecutorial authorities to adduce as evidence material compulsorily obtained by the Ombudsman.

139. Further, the regime contained in Chapter 4A will strengthen oversight and accountability of agency access to stored communications and telecommunications data. The proposed offences and their abrogation of relevant privileges provide support for an effective oversight regime.

140. The disclosure of information to the Ombudsman, and the ability to prosecute a person involved in wrongdoing under the TIA Act, forms a core part of the inspection and oversight functions of the Ombudsman. This function would be significantly impaired if persons were excused from providing self-incriminating information, or if that information could not be used as evidence in TIA Act proceedings.

Other laws do not prevent the disclosure of information for the purposes of an inspection

141. Proposed subsections 186D(3) and (4) will provide that the unlawful disclosure provisions in sections 133, 181A, 181B or 182 of the TIA Act or in any other law will not prevent the disclosure of information to an inspecting officer of the Ombudsman for the purposes of an inspection under the oversight provisions contained in new Chapter 4A.

142. The purpose of provisions such as those in sections 133, 181A, 181B or 182 of the TIA Act is to protect the privacy of impact on persons whose information was accessed under the TIA Act. Given the purpose of the oversight regime in ensuring that agencies access this privacy sensitive information in a lawful manner, it is appropriate that the requirement to disclose information to the Ombudsman under section 186D overrides other laws that would otherwise prevent the disclosure of that information.

The way in which retention of data promotes the right to a fair trial

143. More broadly, the right to a fair trial is promoted by the data retention measures in the Bill on the basis that telecommunications data is equally capable of providing exculpatory evidence as evidence implicating a person in criminality. Accordingly, the potential future lack of availability of key telecommunications data in the absence of this measure may prejudice the right to a fair trial guaranteed by Article 14 of the ICCPR. Given its forensic value, telecommunication data has important evidentiary value in criminal proceedings. The courts have an increasing expectation that such material will be equally available to both the prosecution and defence.

Right to freedom of expression—Article 19 of the ICCPR

144. Article 19 of the ICCPR provides that all persons shall have the right to freedom of expression. This right includes the freedom to seek, receive and impart information and ideas of all kinds, through any media of a person's choice. It has been interpreted as encompassing every form of subjective ideas and opinions capable of transmission to others, and should not be construed as being confined to means of political, cultural or artistic expression.[7] The means of communication listed in Article 19(2) are not exhaustive and the right to freedom of expression has been interpreted as including means of communication such as the contents of phone conversations.[8] Article 19(3) provides that the right to freedom of expression may be subject to restrictions for specified purposes provided in the right, including the protection of national security or public order (*ordre public*, which includes prevention of disorder and crime) where such restrictions are provided by law (that is, set down in formal legislation or an equivalent unwritten norm of common law) and are necessary for attaining one of these purposes.

145. The requirement of necessity implies that any restriction must be proportional in severity and intensity to the purpose sought to be achieved. Limitations on freedom of expression on the grounds of *ordre public* include limitations for the purpose of preventing crime. In order for the proposed laws to be considered a necessary restriction on freedom of expression on the grounds of *ordre public*, the restriction must be clearly defined.

146. The Bill engages the right to freedom of expression in Article 19 to the extent that requiring providers of telecommunications services to retain telecommunications data about the communications of its subscribers or users as part of a mandatory dataset may indirectly limit the right to freedom of expression, as some persons may be more reluctant to use telecommunications services to seek, receive and impart information if they know that data about their communications will be stored and may be subject to lawful access.

147. The proposed data retention regime aims to prevent criminal activity by ensuring that law enforcement and intelligence agencies have access to a limited range of vital telecommunications data, central to virtually every organised crime, counter-espionage, cyber-security and counter-terrorism investigation. It is also used in almost every serious criminal investigation, such as murder, rape and kidnapping. The provisions in the Bill therefore fall within the scope of a specified purpose for which the freedom of expression may be limited.

---

[7] *Ballantyne, Davidson, McIntyre v. Canada*, Human Rights Committee Communications Nos. 357/1989 snf 385/1989 at 11.3.

[8] *J.R.T and the W.G Party v Canada*, Human Rights Committee Communication No 104/1981, 8.

148. To the extent that the measures in the Bill have the effect of limiting the right to freedom of expression, the limitation is designed for the legitimate objective of protecting public order. The Bill limits the extent to which the right to freedom of expression is abrogated by ensuring that only the minimum necessary types and amounts of telecommunications data are retained, and by limiting the range of agencies that may access telecommunications data.

149. The additional safeguards on the access to and use of telecommunications data under the Bill (through limiting the number of enforcement agencies able to access data, making eligibility of access subject to ministerial declaration and the comprehensive Ombudsman oversight of data access and usage in new Chapter 4A) together with existing safeguards under the TIA Act (including that agencies may only request data where it is reasonably necessary for a legitimate investigation) provides assurance that specified data is only retained and used for law enforcement and investigative purposes, meaning that any indirect limitation on the right to freedom of expression in Article 19 is appropriately minimised.

Right to life and security of the person—Articles 6 and 9 of the ICCPR

150. The right to security of the person in Article 9 of the ICCPR requires States to provide reasonable and appropriate measures, within the scope of those available to public authorities, to protect a person's physical security.

151. The right to life also imposes a positive obligation to protect life in Article 6 of the ICCPR. In addition to protecting individuals from unwarranted actions by the State, it is necessary for the State to protect individuals from unwarranted actions by private persons. The Human Rights Committee has confirmed that protection of the right to life 'requires that States adopt positive measures'[9] and the positive obligation to protect life in the context of law enforcement is likely to extend beyond putting in place an effective criminal justice system.[10] Specifically, European jurisprudence has established that the obligation to protect life also requires the police and other protective authorities to take, in certain well-defined circumstances, preventative operational measures to protect an individual whose life is at risk from the acts of a third party.[11] The statutory obligation which the Bill places on service providers to retain a limited subset of telecommunication data which has been determined to be integral for law enforcement and security purposes buttresses the right to life in Article 6 of the ICCPR. If such data is not retained, and law enforcement investigations are resultantly compromised, the ability of police to protect the physical security of potential victims of a crime is critically undermined.

152. Access to telecommunications data at the inception of investigations enables agencies to narrow down the field of initial suspects and to identify linkages, networks and patterns of criminality. It is also the least privacy intrusive methodology to remove alleged suspects from inquiries, and to identify criminal networks. Access to this data is a key building block for investigations, facilitating discovery of and providing context to identities, location and point in time and, potentially, to prevent the commission of further crime. The ability of law enforcement officers to harness investigative mechanisms facilitated by data access, assists in promoting the welfare and safety of potential and actual victims of serious crimes as well

[9] Human Rights Committee, General Comment No 6 (1982), para 5.
[10] *Osman v United Kingdom* (1998) 29 EHRR 245, para 115.
[11] *Osman v United Kingdom* (1998) 29 EHRR 245; see also *Kontrová v Slovakia* [2007] ECHR 7510/04 (31 May 2007). See also *Smith v Chief Constable of Sussex Police* [2008] EWCA Civ 39 (5 February 2008).

as safeguarding the general public who may otherwise be susceptible to security incidents and criminal acts, resulting in the arbitrary deprivation of life.

Summary

153. Any interference with Convention rights occasioned by this Bill is in pursuit of a legitimate aim—the ability of law enforcement and intelligence agencies to obtain telecommunications data in order to safeguard national security, prevent and detect crime and protect members of the public. Access to this telecommunications data is essential for law enforcement and security agencies to effectively investigate a range of criminal offences and threats to national security. In the absence of these measures, there is a risk that agencies will not receive vital information relevant to these investigations. This would limit agencies' abilities to fulfil their obligations into preventing, detecting and prosecuting offences under Australian law and safeguarding Australia's national security. Telecommunications data is not the only source of information available to law enforcement and national security agencies, however it is a critical investigative tool that agencies use in order to identify and prosecute criminals, and protect Australians.

154. It is notable that telecommunications data also plays an important role in protecting the privacy of innocent parties who come within the scope of an agency's investigation, by allowing an agency to rule them out from suspicion at an early stage and without having to resort to more privacy-intrusive investigative methods. For example, call charge records can show that a potential person of interest has had no contact with other members of a criminal syndicate.

155. Telecommunications data is also frequently used to refine and direct the use of more intrusive investigative methods, such as telecommunications interception, avoiding unnecessary invasion of privacy. The ability of law enforcement and national security agencies to use telecommunications data at the early stages of an investigation also displaces the need for agencies to employ more privacy and rights intrusive alternative investigative methods to build a picture of a suspect and their network of criminal associates.

156. Under existing provisions under the TIA Act, law enforcement and national security agencies can only access telecommunications data in limited circumstances. Authorising officers must be satisfied on a case-by-case basis that the disclosure of the information is reasonably necessary, and must consider the impact on privacy when making an authorisation.

157. Any purported interference with Convention rights resulting from this Bill are in pursuit of a legitimate aim, namely the ability of law enforcement and intelligence agencies to access telecommunications data in order to safeguard national security and prevent and detect, investigate and prosecute crime. The reasonableness of the measures and their proportionality is supported by the specificity of the provisions, being appropriately targeted for that legitimate purpose.

158. The additional oversight by the Ombudsman contained in Schedule 3 to the Bill and the limitations on the range of agencies who may access telecommunications data (which will in effect reduce the number and range of agencies able to access this information, and subject the nature of their investigative activities and need for data to greater scrutiny) are

both important safeguards that go towards the reasonableness and proportionality of the new legislation as a whole.

Conclusion

159. The Bill is compatible with human rights because it promotes a number of human rights. To the extent that it may also limit human rights, those limitations are reasonable, necessary and proportionate.

NOTES ON CLAUSES

Clause 1—Short title

160. This clause provides that when the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 is enacted, it is to be cited as the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2014*.

Clause 2—Commencement

161. Clause 2(1) sets out when various provisions of the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2014 (the Act) are to commence, as described in the table.

162. Item 1 in the table provides that sections 1 to 3, which concern the formal aspects of the Act, as well as anything not elsewhere covered by the table, will commence on the day the Act receives the Royal Assent.

163. Item 2 in the table provides that Schedule 1, Items 1 to 7, which amend the Telecommunications (Interception and Access) Act 1979 (the TIA Act) to introduce a mandatory data retention scheme for telecommunications service providers, will commence the day after the end of the period of 6 months beginning on the day this Act receives the Royal Assent. The reason for the delay in commencement of these Items is to ensure that, prior to commencement, service providers can put in place implementation arrangements to comply with the new data retention regime. The delay will also ensure that all appropriate instruments required under the Act are in effect.

164. Item 3 in the table provides that Schedule 1, Items 8 to 11 will commence on the day the Act receives the Royal Assent. Items 8 to 11 in Schedule 1 are application provisions that allow service providers to keep documents and to make applications contained in new Part 5-1A of the Act before that Part commences. These provisions will enable implementation plans and exemptions to be in place upon the commencement of the main amendments, and allow service providers to begin complying with their data retention obligations.

165. Item 4 in the table provides that Schedules 2 and 3 will commence the day after the end of the period of 6 months beginning on the day this Act receives the Royal Assent. The reason for the delay in commencement of these schedules is to enable agencies and oversight bodies to put in place implementation and necessary transition arrangements prior to commencement of the Act.

166. Clause 2(2) will allow the date the Act receives the Royal Assent to be inserted into the Act on publication. This provision will allow specification of the start and end dates for the implementation periods included in Schedules 1 (Items 1 to 7) and Schedules 2 and 3 of the Act.

Clause 3—Schedules

167. Clause 3 provides that each Act specified in a Schedule to this Act will be amended or repealed as set out in the applicable items in the Schedule. Any other item in a Schedule to this Act has effect according to its terms. This is a technical provision to give operational effect to the amendments contained in the Schedules.

SCHEDULE 1—DATA RETENTION

PART 1—MAIN AMENDMENTS

Overview of measures

168. Part 1 of Schedule 1 will insert new Part 5-1A into Chapter 5 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). Chapter 5 deals with the interaction between agencies and carriers.

169. This Schedule will require service providers to retain the telecommunications data prescribed by the regulations.

170. The amendments will provide for:

a. the obligation to keep information and documents (Division 1)

b. data retention implementation plans (Division 2)

c. exemptions from the data retention requirements (Division 3)

d. the confidentiality of data retention implementation plans and exemptions (Division 4)

e. pecuniary penalties and infringement notices (Division 4)

f. a review of the operation of the data retention scheme by the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) no more than 3 years after the end of the implementation phase (Division 4), and

g. annual reporting on the operation of the data retention scheme (Division 4).

171. Mandatory data retention will require service providers to keep a minimum subset of telecommunications data (also known as metadata) that is critical to law enforcement and national security investigations, and will specify the minimum period for which it must be kept. Data retention will create a consistent obligation for record-keeping across the telecommunications industry. The minimum obligation imposed by this legislation is consistent with the types of data and subscriber information currently held by service providers for billing, quality assurance and other business purposes. Some service providers may initially need to modify their systems to ensure they meet this minimum standard.

172. The requirements on service providers to keep data, as provided for by the new Division 1 of new Part 5-1A, will ensure the availability of a set of critical data for law enforcement and national security purposes.

173. New Division 2 of new Part 5-1A will allow service providers to develop and submit implementation plans to the Communications Access Co-ordinator (the CAC) for approval. These plans will set out how the provider will achieve compliance with their data retention obligations over a period of up to 18 months.

174. The implementation plan process is intended to:

- allow service providers to develop and implement more cost-effective solutions to their data retention obligations by, for example, aligning the implementation of such solutions with a provider's internal business planning and investment cycles,
- ensure that service providers achieve substantial compliance with their data retention obligations early in the implementation phase by encouraging interim data retention solutions, such as by increasing the storage for existing databases to allow for a longer retention period, albeit for a period that is less than 2 years, or by implementing full data retention capability for one or more (but not all) services covered by the plan, or for one or more (but not all) kinds of data prescribed in the regulations,
- facilitate engagement between industry and Government on the above issues, and
- provide regulatory certainty for both industry and agencies during the implementation phase.

175. Once approved by the CAC, a service provider will be required to comply with the implementation plan, for a period of up to 18 months, instead of the data retention obligations under new sections 187A and 187C. Additionally, once approved, a plan will only be able to be varied with the consent of the CAC and the service provider.

176. New Division 3 of new Part 5-1A will provide that the CAC may grant exemptions to service providers for any or all of the mandatory data retention obligations. The CAC will be required to consider both the interests of law enforcement and national security agencies, and the objects of the Telecommunications Act 1997 (the Telecommunications Act) when deciding whether to grant an exemption. This will allow exemptions to be granted where, for example, telecommunications data relating to the relevant service is likely to be of little or no relevance to law enforcement or national security investigations, or where the cost of complying, either in full or in part, with data retention obligations in relation to the relevant service would be disproportionately high.

177. New Division 4 of new Part 5-1A will provide that the CAC must treat applications for implementation plans and exemptions as confidential, as must any person to whom the CAC discloses such applications. Division 4 will also provide that the contravention of data retention obligations under Part 5-1A attracts civil penalties. Division 4 will also require the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) to review the operation of the data retention regime three years after mandatory data retention is fully implemented and require the Minister to report on the operation of the data retention regime as part of the annual report on the TIA Act.

Telecommunications (Interception and Access) Act 1979

Item 1—New Part 5-1A

178. Item 1 will insert new Part 5-1A after Part 5-1 of the TIA Act. The provisions to be inserted by this new Part contain the requirements for the retention of prescribed telecommunications data by telecommunications service providers.

Division 1 of Part 5-1A—Obligation to keep information and documents

New section 187A—Service providers must keep certain information and documents

179. This section will provide that service providers must keep prescribed information and documents.

Subsection 187A(1)—Information and documents to be kept

180. Telecommunications data is not defined in the TIA Act. This approach is consistent with the technology-neutral approach of the Privacy Act, and Part 13 of the Telecommunications Act.12 The term is described, however, through the provisions of Divisions 3, 4 and 4A of Chapter 4 of the TIA Act , which contain the powers of agencies to make authorisations for the disclosure of information or documents protected under Part 13 of the Telecommunications Act, and section 172 of the Act, which provides that Divisions 3, 4 and 4A do not permit the disclosure of information that is the contents or substance of a communication, or a document to the extent that it contains such information. As such, telecommunications data can be considered to be information about a communication, but not its content or substance.

181. Data retention obligations will not apply to all telecommunications data.

182. The purpose of the proposed data retention obligation is to create a consistent minimum retention obligation across the telecommunications industry in relation to a limited range of telecommunications data that is critical to law enforcement and national security investigations. Data retention obligations will apply, pursuant to subsection 187A(1), to information of a kind prescribed by the Governor-General in regulations, or documents containing such information, relating to a service operated by the service provider for the period specified under new section 187C. This regulation-making power is subject to limits set out in subsections 187A(2), (3) and (6). Subsection 187A(3) describe the services to which data retention obligations apply.

183. A regulation-making power is required to ensure that the legislative framework gives service providers sufficient technical detail about their data retention obligations while remaining flexible enough to adapt to future changes in communication technology.

Subsection 187A(2)—Only certain kinds of information to be prescribed

184. Subsection 187A(2) limits the scope of the regulation-making power under subsection 187A(1) by providing that the kinds of information that may be prescribed in regulations under paragraph 187A(1)(a) must relate to certain categories of information. Each of these categories of information is of significant utility to law enforcement and national security investigations. The scope of the regulation making power is limited to the six categories of information prescribed in subsection 187A(2). The types of data that may be prescribed are circumscribed to remain necessary and proportionate to the legitimate aim of ensuring that law enforcement and intelligence agencies have access to the critical data they require to safeguard national security and prevent or detect criminal activity.

[12] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 73.33.

The table below sets out the kinds of information listed in subsection 187A(2), along with a description of the information that may be included within each kind of information, and an accompanying explanation. This table is not exhaustive of the information that may be included within each kind of information listed in subsection 187A(2).

Information or documents to be kept

Para	Kind of information	Description of information that may be included	Further explanation
(a)	Characteristics of any of the following:		This paragraph lists kinds of information that may be prescribed relating generally to subscriber administration information held by the provider.
(a)(i)	Characteristics of a subscriber of a relevant service	Information that is: • name • address information • other information used for identification purposes • billing and payment information, or • contact information relating to the relevant service.	The word 'subscriber' refers to a person who is a customer or account holder of the service, and could include additional authorised or registered users. This category may include both present and past subscriber name and address information (including residence, business, post office, billing, payment or installation addresses). This may also include additional information, such as identification information, date of birth, financial, charging, billing and payment information, other transactional information, or contact information. Service providers are not required to collect and retain passwords, PINs, secret questions or token codes, which are used for authentication purposes.
(a)(ii), (iii) & (iv)	Characteristics of an account, telecommunications device or other relevant service relating to a relevant service	Information about an account, telecommunications device, or other relevant service that is or has been associated with a relevant service, which may include: • any information relating to contracts, plans, agreements or arrangements relating to the relevant service, or to any related account, service or device	This category may cover characteristics of accounts such as the particular 'deal' or 'bundle' that a customer has signed up to and any upgrades or features that apply to the service.

Information or documents to be kept			
Para	**Kind of information**	**Description of information that may be included**	**Further explanation**
		• any identifiers, either permanent or transient, that the service provider uses in relation to the account, device or relevant service	Service providers regularly allocate identifiers to an account, device or relevant service which are then used in relation to the provision of the relevant service. Service providers also use identifiers allocated by others, such as device manufacturers. These identifiers may include, for example, a user name, email address, or International Mobile Subscriber Identity (IMSI). This category may also include Internet Protocol (IP) addresses, port numbers or other network identifiers which may be used on a permanent or transient basis. A service provider may also be required, in relation to this category, to retain multiple identifiers. For example, if a service provider uses Network Address Translation across its network or service, the service provider may be required to keep records relating to each set of identifiers to link the account, device or relevant service to a subscriber.
		• the status of the relevant service or any related account, service or device, and	This may include any change in the account state or billing type, such as information about an account being suspended due to a failure to pay, or about the pre-paid status of a service, or about a device provided as part of a plan to which a person has subscribed. 'Status' should not be read to include the transient or operational status of a device, such as if it is currently in use, fully charged or turned off.
		• any quantitative data about the capacity or use of the account of the relevant service or a related account, service or device.	This kind of information may include any metrics that describe the account or such as its available talk minutes, bandwidth, upload and/or download volumes. This category may also capture similar kinds of information about how an account, service or device has been used. 'Use' should not be read broadly to include non-aggregated information about particular communications or matters specifically excluded such as web browsing history.

Information or documents to be kept			
Para	**Kind of information**	**Description of information that may be included**	**Further explanation**
(b)	The source of a communication	Any identifiers of a related account, service or device from which a communication has been sent or attempted to be sent by means of the relevant service. This may include any identifier or combination of identifiers which are used by the service provider to describe the account, service and/or device at the time of the successful or attempted communication.	Paragraph 187A(3)(b) puts beyond doubt that the regulation-making power cannot be used to require service providers to keep information about subscribers' web browsing history. An example of an identifier of the source of a communication is a telephone number. This kind of information may include information about the source of a communication that originated on another provider's network or service. Where one or more source identifiers are passed from the other provider's network or service to the relevant provider's network or service, those source identifiers may be included in the information that the service provider is required to keep. This kind of information may include identifiers allocated to an account, telecommunications device or service for communications originating from another provider's network or service, to the extent that such identifiers are visible or available to the service provider operating the relevant service. For instance, if a phone on one network calls a phone on a second network, the operator of the second network may be required to keep the number of the phone that originated the call from the first network.
(c)	The destination of a communication	Any identifiers of the account, telecommunications device or service (other than the relevant service) and device to which the communication:	Paragraph 187A(3)(b) puts beyond doubt that the regulation-making power cannot be used to require service providers to keep information about subscribers' web browsing history.

Information or documents to be kept			
Para	**Kind of information**	**Description of information that may be included**	**Further explanation**
		• has been sent or attempted to be sent, or	This kind of information may include any identifier transmitted to a network or service to cause (or attempt to cause) a communication to take place. An example of such an identifier is the telephone number dialled when making a telephone call. This kind of information may include any identifiers allocated to an account, telecommunications device or service to which a communication is sent. An example would be the identifiers of an email server used to deliver an email to its recipient/s. Another example is where call forwarding/diversion is applied. The information regarding the originally intended destination and the newly routed destination could be required to be kept. This kind of information may include identifiers allocated to an account, telecommunications device or service for communications terminating on another provider's network or service, to the extent that such identifiers are visible or available to the service provider operating the relevant service. For instance, if a phone on one network calls a phone on a second network, the operator of the first network may be required to keep the number of the phone that received the call on the second network.
		• has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.	Examples of this kind of information may include: • for a Voice over Internet Protocol (VoIP) service, the identifiers generated by the network or service when translating the VoIP phone number or account name dialled by the caller into an IP or other network address • the number to which a call was forwarded • a voicemail short-dial to full number translation, or • a 13, 1300, 1800 prefixed number to other termination number translation.

Information or documents to be kept			
Para	**Kind of information**	**Description of information that may be included**	**Further explanation**
(d)	The date, time and duration of a communication, or of its connection to a carriage service	The time and the date of the following relating to the communication: • the start of the communication • the end of the communication • the connection to the relevant service, and • the disconnection from the relevant service.	This kind of information may include information required to determine the time at which a communication commenced and concluded, or at which a subscriber or device connected and disconnected from the relevant service. An example of this may be a username combined with the time it was used, with the time expressed in Coordinated Universal Time (UTC) with the appropriate time offset (eg 20:00 UTC +2:00) . A service provider may be required to keep such information with a sufficient degree of accuracy to allow a link to be made between a communication or connection and the account, telecommunications device or relevant service to or from which the communication was sent. The degree of accuracy that may be required may vary between services. For example, if a particular service frequently reallocates transient identifiers to accounts, telecommunications devices or relevant services, the service provider may be required to ensure that time and date information is sufficiently accurate to reliably link a particular communication or connection with the account, telecommunications device or relevant service to or from which the communication was sent.
(e)	The type of a communication and relevant service used in connection with a communication	The type of communication. The type of service.	This is the product or service that is made available to a user by the service provider. For example, whether the service or product provided is email, internet access, mobile telephony services or mobile phone text messaging such as Short Message Services (SMS). For application services provided over the top of internet access, examples of service types include Voice over Internet Protocol (VoIP), instant messaging or email. For services that provide access to a network or the internet, examples of service types include symmetric digital subscriber line (ADSL) or frequency division Long-Term Evolution (FD-LTE).

Information or documents to be kept			
Para	**Kind of information**	**Description of information that may be included**	**Further explanation**
		The features of the relevant service that were, or would have been, used by or enabled for the communication.	Examples include voicemail, call waiting, and bandwidth allocation.
(f)	the location of equipment or a line used in connection with a communication	The physical and logical location of the line, equipment or telecommunications device used to send or receive a communication.	Subsection 187A(1) will provide that a service provider must keep prescribed information relating to any communication carried by means of the relevant service. Subsection 187A(1) therefore does not require a service provider to keep information about the location of a line, equipment or telecommunications device when it is not communicating, such as information about the location of a mobile device that is not being used to send or receive a communication.[13] Examples include cell tower locations and public wireless local area network (WLAN) hotspots. The obligation may require providers to retain sufficient historical information about the location of towers and hotspots to ensure location information remains interpretable over the course of the retention period.

Subsection 187A(3)—Application of Part 5-1A to certain services

185. Subsection 187A(3) will set out the services to which the data retention obligations under Part 5-1A of the Act will apply. Data retention obligations will only apply to services that satisfy paragraphs 187A(3)(a), (b) and (c).

186. Paragraph 187A(3)(a) will provide that the Part applies to a service if it is a service for carrying communications, or that enable communications to be carried, by guided or unguided electromagnetic energy or both. Section 5 of the TIA Act defines the term 'carry' for the purposes of the TIA Act. The term is defined in the same manner as in the Telecommunications Act, but should be interpreted in light of the objective of the TIA Act to allow for lawful access to communications in relation to law enforcement and national security investigations. The concept of 'enabling' a communication to be carried is intended to put beyond doubt that data retention obligations apply to relevant services that operate 'over the top' of, or in conjunction with, other services that carry communications.

[13] See also subsection 187A(8), which will put beyond doubt that the regulation-making power cannot be used to require service providers to keep records about the location of a line, equipment or telecommunications device on a continuous basis throughout a single communications session, such as an internet access session.

187. Paragraph 187A(3)(b) will provide that the Part applies to a service if it is:

a. operated by a carrier (within the meaning of the TIA Act);

b. operated by an internet service provider (within the meaning of Schedule 5 of the *Broadcasting Services Act 1992*).; or

c. prescribed in regulations.

188. A service will be 'operated by' a carrier or an internet service provider even if:

a. the service itself would not require a carrier licence, or the service is not a 'carriage service' (within the meaning of the Telecommunications Act); for example, if a licenced carrier operates an email service, that service will still be operated by the carrier notwithstanding that to provide an email service does not require a licence; or

b. in the case of an internet service provider, the service itself is not an 'internet access service' (within the meaning of Schedule 5 of the *Broadcasting Services Act 1992*); for example if a internet service provider operates a VoIP service, that service will still be operated by the internet service provider notwithstanding that a VoIP service is not itself an internet access service.

189. The telecommunications industry is highly innovative and increasingly converged. Sophisticated criminals and persons engaged in activities prejudicial to security are frequently early adopters of communications technologies that they perceive will assist them to evade lawful investigations. As such, a regulation-making power is required to ensure the data retention regime is able to remain up-to-date with rapidly changes to communications technologies, business practices, and law enforcement and national security threat environments.

190. Paragraph 187A(3)(c) will provide that Part 5-1A applies to a service if the person operating the service owns or operates, in Australia, infrastructure that facilitates, or relates to, the provision of any of its services, of a kind referred to in paragraph (a). The term infrastructure should be given its natural meaning within the context it appears. The intention of paragraph 187A(3)(c) is that Part 5-1A will apply to a service if the person operating the service owns or operates infrastructure in Australia relating to any of its services, irrespective of whether the person owns or operates infrastructure in Australia relating to the particular service in question.

191. Data retention obligations will not, however, apply to a broadcasting service (within the meaning of the *Broadcasting Services Act 1992*). The definition of a 'telecommunications service' in section 5 of the TIA Act currently excludes a service for carrying communications solely by means of radiocommunication. This exclusion is appropriate for the purposes of prohibiting and regulating the lawful interception of telecommunications, where it is appropriate to consider the end-to-end passage of a communication across a telecommunications system (as defined in section 5 of the TIA Act). Data retention obligations, by comparison, expressly relate to such parts of a telecommunications service or system as are operated by a given service provider and which may, therefore, involve a service for carrying communication solely by means of

radiocommunication. As such, subsection 187A(3) does not incorporate the radiocommunications exception, but excludes broadcasting services.

Subsection 187A(4)— Information not required to be kept

192. Paragraph 187A(4)(a) will provide that service providers will not be required to keep information or documents that are the contents or substance of a communication, such as the words spoken during a phone call, or an email subject line. This paragraph gives effect to the relevant part of recommendation 42 of the PJCIS in its *Report of the inquiry into potential reforms of Australia's national security legislation* (the PJCIS Report) that any mandatory data retention regime should apply only to telecommunications data and exclude content. The paragraph explicitly states that the obligation to keep information does not require a carrier to retain content.

193. Paragraph 187A(4)(a) will not preclude carriers from retaining the content or substance of a communication for other lawful purposes, such as their lawful business purposes. For example, a service provider that provides an email service may keep the content of emails on a server as an inherent part of providing that service.

194. Section 172 of the TIA Act currently prohibits ASIO or enforcement agencies from authorising the disclosure of the substance or content of a communication under a data authorisation made under Chapter 4 of the TIA Act. Agencies may only access the substance or content of a communication under a warrant, or in limited other circumstances, such as in a life-threatening emergency.

195. Paragraph 187A(4)(b) will provide that service providers will not be required to retain information or documents that state an address to which a communication was sent on the internet from a telecommunications device using an internet access service provided by the service provider, and that was obtained by the carrier only as a result of providing a service for internet access.

196. This provision gives effect to the relevant part of recommendation 42 of the PJCIS Report, that internet browsing data should be explicitly excluded from the scope of any mandatory data retention regime. This provision will go further than the PJCIS Report recommended by ensuring that service providers are not required to keep records of the uniform resource locators (URLs), internet protocol (IP) addresses, port numbers and other internet identifiers with which a person has communicated via an internet access service provided by the service provider. The provision is required because a URL will in some cases be telecommunications data rather than content.

197. Paragraph 187A(4)(b) will only apply, however, to internet address identifiers obtained by a carrier solely as the result of providing an internet access service. If the service provider obtains a destination internet address identifier as the result of providing another service, the provider will be required to keep a record of that identifier. For example, an email service provider will be required to keep records of the destination internet address identifiers associated with the use of an email service, such as the email and IP address, and port number to which an email was sent. Similarly, if a service provider that provides an internet access service to a subscriber also provides a Voice over the Internet Protocol (VoIP) service to that subscriber, the service provider will be required to keep records of any destination internet address identifiers associated with the use of that VoIP service. This could include the internet protocol (IP) address to which a VoIP call was sent. In this

example, however, the service provider will continue to not be required to keep records of any other destination internet address identifiers associated with web browsing.

198. Paragraph 187A(4)(b) operates to exclude information of a certain character from retention obligations—being information an internet access service provider has about destinations on the internet that the provider only has because it provides that service. While internet access services are used to both send and receive information, received information is still of the above character and excluded by the paragraph. However, this paragraph does not exclude any provider from retaining information about the identifiers it assigns, on a permanent or transient basis, to an account, device or relevant service, such as network address translation (NAT) information.

199. Paragraph 187A(4)(b) is not intended to preclude the retention of IP addresses or port numbers allocated to a subscriber, or a communication or a device by the service provider. That information can be required to be retained by subsection 187A(2)(b).

200. Paragraph 187A(4)(c) will provide that the requirements to keep data under section 187A will not apply to data about a communication that has been carried by means of another relevant service operated by another service provider, but which is using the relevant service operated by the service provider. The purpose of this provision is to ensure that the provider of an underlying service, such as an internet access service, is not required to keep information about communications that are passing 'over the top' of the underlying service and that are being carried by means of another relevant service, such as a VoIP service, operated by another provider. This exception only applies, however, to the extent that it relates to such a communication. In the above example, the provider of the underlying internet access service could be required to retain information including information about the subscriber to the internet access service (subparagraph 187A(2)(a)(i)), and the date and time at which the subscriber connected and disconnected from the internet access service (paragraph 187A(2)(d)), subject to prescription of that data by regulation.

201. Paragraph 187A(4)(d) will provide that the requirements to keep data under section 187A will not apply to information that a service provider is required to delete because of a determination made under section 99 of the Telecommunications Act. An example of such a determination is the *Telecommunications (Service Provider—Identity Checks for Pre-paid Public Mobile Carriage Services) Determination 2013*.

202. Paragraph 187A(4)(e) will provide that a service provider is not required to keep information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected. This could include, for example, a record of which cell tower, base station or other network access point a device was connected to. This provision will ensure, however, that service providers are not required to generate and keep location records that are more detailed than or different to the location records used in relation to the relevant service.

Subsection 187A(5) —Attempted and untariffed communications

203. Paragraph 187A(5)(a) will provide the circumstances in which an attempt to send a communication is taken to be the sending of a communication, which would trigger data retention obligations under subsection 187A(1). These circumstances would include, for example, where:

a. a phone number is dialled, but the phone rings and is unanswered or rings out (subparagraph 187A(5)(a)(i))

b. an email server attempts to send a new email to an email client, but the client email server does not exist or is not working (subparagraph 187A(5)(a)(ii)), or

c. a mobile phone number is dialled, but the destination mobile phone is switched off and so is not recorded on the network's Visitor Location Register; as such, the network does not attempt to connect the phone call and instead informs the caller that the phone is switched off or unavailable (subparagraph 187A(5)(a)(iii)).

204. Paragraph 187A(5)(b) will clarify that untariffed communications, such as 1800 phone calls, communications sent using 'unlimited' phone or internet plans, or free internet or application services, are communications for data retention purposes, and thus may be the subject of data retention obligations.

Subsection 187A(6)—Service providers must create information or a document if not already created by the operation of the relevant service

205. Subsection 187A(6) will clarify that if the information or documents that service providers are required to keep under subsection 187A(1) are not created by the operation of the relevant service, or if they are only created in a transient fashion, then the service provider is required to use other means to create this information or document.

206. Mandatory data retention is the creation of a consistent minimum standard across the telecommunications industry for what data is to be collected and how long it is to be retained. Subsection 187A(6) will ensure that all service providers must meet this minimum standard, whether or not that data is currently being collected or retained by the relevant service provider.

Subsection 187A(7)—Two or more communications taken to be a single communication

207. Subsection 187A(7) provides that for the purposes of certain information or documents required to be kept under paragraphs 187A(2)(b), (c), (d) and (f), two or more communications that together constitute a single communications session are taken to be a single communication.

208. The purpose of subsection 187A(7) is to ensure that providers are not required to record the source, destination, time, date and duration of a communication or the location of a device throughout a communications session. The definition of 'session' intends to prevent the data retention obligation applying to every packet. Instead, it allows multiple communications to be constructed into a single session so they are more analogous to their traditional counterparts. For instance, even though a VoIP call is constructed from many packets, each call should be considered a single session in the same way that a traditional telephone call would be considered a single communication.

209. For example, a smartphone connected to a mobile data network may have multiple applications running in the background, each of which may routinely communicate with remote servers, such as to seek and obtain updates. As such, the smartphone may send and receive a near-continuous stream of communications. However, these communications may

together constitute a single communications session. Absent this provision, providers could, for example, be required to record the location of the device on a near-continuous basis. The effect of the provision is that providers will only be required to record prescribed location information for the overall communication rather than its constituent components.

210. Whether a series of communications constitutes a single communications session is a question of technical fact and will depend upon the objective operation of the provider's network or service. This question should not be determined from the user's perspective, as the provider subject to data retention obligations will generally be unable to assess a user's intentions in this regard, and in many cases, users are unlikely to be aware of when their device is communicating, such as when applications installed on a smartphone or computer are automatically seeking and receiving updates.

New section 187B—Certain service providers not covered by this Part

211. Section 187B will exclude certain service providers from being required to comply with data retention obligations under new subsection 187A(1) of the TIA Act. The purpose of proposed section 187B will be to ensure that entities such as governments, universities and corporations will not be required to retain telecommunications data in relation to their own internal networks (provided these services are not offered to the general public), and that providers of communications services in a single place, such as free Wi-Fi access in cafes and restaurants are not required to retain telecommunications data in relation to those services. However, the CAC can declare that data from such services must nevertheless be retained.

212. Subparagraph 187B(1)(a)(i) will provide that data retention obligations do not apply if the service is provided only to a person's 'immediate circle' within the meaning given by section 23 of the Telecommunications Act. This definition includes (amongst other things) persons in corporate networks, government networks and tertiary institutions. Such networks will be excluded from data retention obligations if the carriage services (as defined in the Telecommunications Act) associated with them are not available to the general public.

213. Subparagraph 187B(1)(a)(ii) will provide that data retention obligations do not apply if the service is provided only to places that are all in the same area, as defined in section 36 of the Telecommunications Act. Section 36 of the Telecommunications Act describes a range of circumstances in which places are considered to be all in the same area. Generally speaking, the concept of 'same area' will include (amongst other things) places such as university campuses, cafes or restaurants.

214. Paragraph 187B(1)(b) will qualify the exemptions in paragraph 187B(1)(a) by providing that the CAC can make a declaration under subsection 187A(2) that data must nevertheless be retained in relation to the relevant services.

215. Subsection 187B(2) will provide that the CAC can declare that the provider of an 'immediate circle' or 'same area' service (as defined in subsection 187B(1)) is nevertheless required to retain telecommunications data in relation to the relevant services according to the requirements of subsection 187A(1).

216. Subsection 187B(3) will provide that in making a declaration under subsection 187B(2), the CAC must take into account the interests of law enforcement and national security and the objects of the Telecommunications Act. The main (but not the only) objects

of the Telecommunications Act are set out in section 3(1) of that Act and are to provide a regulatory framework that promotes:

a. the long-term interests of end-users of carriage services or of services provided by means of carriage services

b. the efficiency and international competitiveness of the Australian telecommunications industry, and

c. the availability of accessible and affordable carriage services that enhance the welfare of Australians.

217. Subsection 187B(4) will provide that the CAC's declaration must be in writing.

218. Subsection 187B(5) will provide that a declaration made by the CAC under this section is not a legislative instrument. Subsection 187B(5) will be included to assist readers, as a declaration made by the CAC under this section is not a legislative instrument within the meaning of section 5 of the *Legislative Instruments Act 2003*.

New section 187C—Period for keeping information and documents

219. Section 187C will set out the required period for service providers to retain specified telecommunications data. A retention requirement of two years is consistent with the aim of the legislation and is necessary having regard to the reasonable requirements of national security and law enforcement agencies to have telecommunications data available for investigations and the privacy of users of the Australian telecommunications system. Experience under the former European data retention scheme was that, while frequently data accessed by agencies was less than six months old, for national security and serious criminal offences, data up to two years old would often be required for the most complex investigations into crimes and threats to national security that can have the most damaging effect.

220. However, the retention period in section 187C will be subject to an exemptions regime to be implemented in proposed Division 3 of Part 5-1A. In particular, paragraph 187K(1)(c) will allow the CAC to reduce the required retention period. In addition, data retention implementation plans that a service provider may provide under proposed Division 2 of Part 5-1A of the TIA Act may also be relevant to the period for which a service provider must retain relevant data. It will be possible for a data retention implementation plan to specify a retention period for a service offered by a service provider of less than two years in relation to services under the plan while the plan is in force.

221. Paragraph 187C(1)(a) will set out the required period for retention of subscriber telecommunications data. Subscriber telecommunications data is the documents or information of the kind described in proposed paragraph 187A(2)(a) and set out in regulations. For basic subscriber data, a service provider must retain the data from when it was created until two years after the closure of the relevant account. Records relating to the use of an account, such as call-charge records, are significantly less useful if they cannot be associated with a real-world subscriber. Subscriber records are typically generated when an account or service is opened, and may not be updated for many years. The purpose of this provision is to ensure that subscriber records associated with an account are available throughout the life of the account, and for as long as records relating to communications sent

using that account are retained. This is intended to ensure that the necessary information is available to establish a connection between a particular communication and the subscriber.

222. Paragraph 187C(1)(a) is subject to subsection 187C(2), which permits the Governor-General to prescribe in regulations that the retention period for certain information of a kind described in paragraph 187A(2)(a) is the period starting when it came into existence and ending two years after the information came into existence.

223. Paragraph 187C(1)(b) will set out the required retention period for all types of data that is required to be retained, other than subscriber data. In general terms, this will include telecommunications traffic data. Specifically, it will mean the information or documents referred to in paragraphs 187A(2)(b)-(f). and set out in the applicable regulations. As the provision provides, the required retention period for this data is from when that data came into existence until two years after it came into existence.

224. Subsection 187C(3) will provide that a service provider is not prevented by the provisions of new section 187C from keeping telecommunications data for longer periods that those set down in section 187C. This means, for example, that service providers will not be prevented by new section 187C from retaining telecommunications data for longer than two years for their own lawful business purposes. Likewise, the scheme does not intend to regulate the de-identification and destruction of data once the retention period has expired. However, other laws/regulations may mandate how providers handle the retained data once the retention period has expired.

225. For instance, the Australian Privacy Principles (APPs), as set out in Schedule 1 of the *Privacy Act 1988* (the Privacy Act), will still apply to service providers covered by the Privacy Act and their dealings with the telecommunications data that is personal information and that is required to be retained under the new Part 5-1A of the TIA Act. For instance, APP 11.2 requires entities to take reasonable steps to destroy personal information or to ensure that the information is de-identified where the entity no longer needs the information for a reason set out in the APPs. Where the required retention period for telecommunications data under the new Part 5-1A of the TIA Act expires, entities may be required to destroy or de-identify such information if it constitutes personal information.

226. However, as APP 11.2(d) provides, an entity is only required to destroy or de-identify personal information where 'the entity is not required by or under an Australian law… to retain the information'. The data retention requirements set out in new Part 5-1A of the TIA Act constitute such a law requiring retention of the relevant information during the specified period.

Division 2 of Part 5-1A—Data Retention Implementation Plans

227. Division 2 of Part 5-1A of the TIA Act will support the development of data retention implementation plans. Data retention implementation plans are intended to be plans that will allow the telecommunications industry to design a pathway to full compliance with their telecommunications data retention obligations within 18 months of the commencement of those obligations, while also allowing for interim measures that result in improved data retention practices.

228. Data retention implementation plans will complement the availability of exemptions under proposed Division 3 of Part 5-1A. For example, a service provider will be able to seek

an exemption for some of its services under Division 3 while at the same time submit an implementation plan for some or all of its other services under Division 2.

New section 187D—Effect of data retention implementation plans

229. Section 187D will set out the effect of data retention implementation plans. While a plan is in force in relation to a relevant service offered by the service provider, the service provider must comply with the plan in relation to that service in lieu of the obligations that would otherwise apply under section 187A.

New section 187E—Applying for approval of data retention implementation plans

230. Section 187E will set out the process for service providers to apply for approval of data retention implementation plans. Submission of implementation plans by service providers is voluntary. However, in the absence of an implementation plan, service providers will be required to comply with the data retention obligations immediately on their commencement.

231. Subsection 187E(1) will provide that a service provider can apply to the CAC for approval of an implementation plan in relation to one or more services that it offers. The application provisions contained in Part 3 will permit applications to be lodged, considered and approved from the date of the Royal Assent. A service provider is not obliged to submit an implementation plan for all of its services.

232. Subsection 187E(2) will set out the matters a service provider's implementation plan must include. The purpose of subsection 187E(2) is to ensure that a service provider's implementation plan gives sufficient information for the CAC and any other person considering the plan to make an informed decision on the plan.

233. Paragraph 187E(2)(a) will provide that a service provider's implementation plan will be required, in relation to each relevant service, to have an explanation of the current relevant data retention practices of the service provider. In particular, paragraph 187E(2)(a) will require the plan to explain what practices the service provider would have in relation to the information or documents it would otherwise have had to retain under section 187A, had the implementation plan not been in force. This will ensure that the CAC has sufficient knowledge of existing practices to ascertain the changes to its practices the service provider will have to undertake to meet its obligations.

234. Paragraph 187E(2)(b) will require that an implementation plan include details of the interim arrangements, if any, that a service provider proposes to implement prior to achieving full compliance. Examples of interim arrangements that a service provider could propose include collection on only part of the data set normally required to be kept under subsection 187A(1) or retention of such data for less than two years. A service provider can propose more than one interim arrangement over the life of the implementation plan for any particular relevant service.

235. Paragraph 187E(2)(c) will specify that a service provider's implementation plan will be required, in relation to each relevant service, to specify when the service provider will comply with its data retention obligations under section 187A and the required time period for retaining relevant information or documents under section 187C. However, as stated in paragraph 187E(2)(c), a service provider will not be required to provide this information in

its plan to the extent that it has obtained relevant exemptions from its data retention obligations from the CAC under Division 3 of Part 5-1A of the TIA Act.

236. Subsection 187E(3) will clarify that a service provider is not able to nominate a date in its implementation plan for compliance with its data retention obligations that is later than the relevant date provided in proposed section 187H regarding when implementation plans are in force. Under subparagraph 187H(b)(i), for telecommunications services that the service provider was already operating when Part 5-1A of the TIA Act commenced, the relevant date is 18 months after commencement of Part 5-1A. Under subparagraph 187H(b)(ii), for telecommunications services that the service provider was not already operating when Part 5-1A of the TIA Act commenced, the relevant data will be 18 months after the time when the service provider started operating the service.

237. Subsection 187E(4) will provide that a service provider's plan must also specify:

- any relevant services of the service provider not covered in the implementation plan; and
- the contact details of relevant employees of service providers in relation to the implementation plan.

238. The purpose of paragraph 187E(4)(a) is to ensure that the implementation plan makes it clear whether relevant services of the service provider are not proposed to be incorporated in the plan. This will provide the CAC, and any other person considering the plan, with information to make an informed decision on the plan.

239. Paragraph 187E(4)(b) will also ensure that the relevant employees of the service provider can be contacted directly in relation to the plan. Service providers should provide names, direct phone numbers and email addresses of staff who have worked on or are responsible for the implementation plan. This provision is designed to avoid, for example, a situation where the CAC or other relevant persons would have to contact the service provider's general public contact number to discuss the implementation plan.

New section 187F—Approval of data retention implementation plans

240. Section 187F will set out the process for the CAC to consider and to approve data retention implementation plans.

241. Subsection 187F(1) will provide that, if a service provider submits a plan to the CAC, the CAC must either approve the plan and notify the service provider, or give the plan back to the service provider for specified amendments. The CAC may not refuse to take the plan or decline to consider the plan.

242. Subsection 187F(2) will set out a list of factors the CAC must take into account in deciding whether or not to approve a plan submitted by a service provider. These factors will be:

- 187F(2)(a)—The desirability of the service provider achieving substantial compliance with its data retention obligations as soon as is practicable (which would take into account any interim arrangements proposed by the service provider, as well as the time by which the provider proposes that each service covered by the plan will be fully compliant).

- 187F(2)(b)—Whether the proposed implementation plan would reduce the regulatory burden on the service provider made by data retention obligations in Part 5-1A.
- 187F(2)(c)—If the service provider is not complying with its data retention obligations in relation to one or more of its services—the reasons why the service provider is not complying.
- 187F(2)(d)—The interests of law enforcement and national security.
- 187F(2)(e)—The objects of the Telecommunications Act. The main (but not the only) objects of the Telecommunications Act, as set out in section 3 of that Act, are:
    - the long-term interests of end-users of carriage services or of services provided by means of carriage services
    - the efficiency and international competitiveness of the Australian telecommunications industry, and
    - the availability of accessible and affordable carriage services that enhance the welfare of Australians.
- 187F(2)(f)—Any other matter the CAC considers relevant.

243. Subsection 187F(3) will provide that, if the CAC does not make a decision and communicate that decision within 60 days, it will be deemed that the CAC has made and notified the service provider of the decision the service provider asked for. The effect of this provision will be to ensure that the service provider is required to comply with the implementation plan in lieu of the obligations that otherwise apply under sections 187A and 187C. This provision will not require the CAC to make a decision within 60 days, rather the provision is intended to ensure that service providers have certainty about their obligations (and are not required to act in an manner that would pre-empt the CAC's decision) in situations where the CAC takes more than 60 days to either approve or to request an amendment to the plan.

244. Subsection 187F(4) will qualify subsection 187F(3). Proposed subsection 187F(4) will provide that a deemed decision under subsection 187F(3) is in force only until the CAC makes and communicates to the service provider the CAC's actual decision on the application.

245. The CAC's decision is not reviewable under the *Administrative Decisions (Judicial Review) Act 1977* (the ADJR Act) as decisions under the TIA Act are not decisions to which the ADJR Act applies (see paragraph (d) of Schedule 1 to the ADJR Act). The exclusion of these decisions from the ADJR Act does not prevent decisions made under the TIA Act from being judicially reviewable under paragraph 75(v) of the Constitution and s 39B of the *Judiciary Act 1901* (Cth).

New section 187G—Consultation with agencies and the ACMA

246. Section 187G will set out the consultation process that the CAC must undertake in relation to data retention implementation plan applications that it receives.

247. References to the 'original plan' in section 187G mean references to the data retention plan originally submitted by the service provider under section 187E of the Act, rather than

to any amended version of the plan created (or proposed to be created) under the processes set out in section 187G.

248. Subsection 187G(1) will provide that, once the CAC receives an implementation plan application, the CAC must give a copy of the plan to the enforcement agencies and security authorities that are likely to be interested in the plan for comment, and may give a copy to the Australian Communications and Media Authority (ACMA).

249. Subsection 187G(2) will govern requests for amendment of a service provider's original plan, providing that if an enforcement agency or security authority makes a request for amendment of the plan, the CAC must consider whether the request is reasonable. If the CAC considers the request is reasonable, the CAC must give the service provider a copy of the request, and may also provide the service provider with a copy of the comment, or a summary of the comment. The CAC must then request the service provider to respond to the CAC within 30 days after receiving the comment or summary.

250. Subsection 187G(2) is intended to ensure that interested enforcement agencies and security authorities have the opportunity to comment on and request amendments to a service provider's proposed implementation plan, and to require the CAC to provide those requests to the service provider, if he or she considers such requests to be reasonable. Subsection 187G(2) will not require the CAC to provide a service provider with a copy or summary of the comment accompanying a request as, in some cases, it will not be appropriate to do so, including where the comment relates to sensitive law enforcement or national security matters.

251. Subsection 187G(3) will provide that a service provider must respond to a request for amendment of its plan that it received under subsection 187G(2). The service provider must either:

- accept the request for amendment by giving the CAC an appropriately amended plan within the 30 day period set out in subsection 187G(2), or
- indicate that it does not accept the request for amendment and provide its reasons to the CAC.

252. In the event that a service provider does not comply with the requirement to respond (either adequately or at all) to the CAC in relation to the request for amendment within the 30 day period, subsection 187G(3) should be interpreted to mean that the service provider is taken not to have accepted the request for amendment. As the deeming provision under subsection 187F(3) ceases to apply once the CAC notifies a service provider of a request to amend a plan, a failure by a service provider to respond to a request for amendment within the required period may result in the service provider being subject to data retention obligations under sections 187A and 187C.

253. Subsections 187G(4) and (5) will provide for the role of ACMA in relation to proposed amendment of a service provider's implementation plan. The purpose of subsections 187G(4) and (5) will be to require the CAC to refer disputes over proposed implementation plan amendments to ACMA for determination by ACMA.

254. Data retention implementation plans will be highly technical documents. The ACMA is the industry regulator for the telecommunications industry, and has substantial expertise relating to the technical and commercial operation of the industry. As such, the ACMA is the

appropriate body to review any dispute over a request to amend a data retention implementation plan.

255. Subsection 187G(4) will apply in the event the service provider does not accept a request for amendment of its plan. If so, the CAC must refer the request for amendment to the ACMA along with the service provider's response (if one was given) and request the ACMA to make a determination on the dispute. Under subsection 187G(5) the ACMA will then be required to determine in writing either that no amendment of the plan is necessary or that that original plan should be amended. The ACMA will only be able to determine that the original plan should be amended if the ACMA considers the amendment request to be reasonable and the service provider's response to the request for amendment to not be reasonable. In the event that the service provider does not respond (or did not respond adequately) under proposed subsection 187G(3), *prima facie* that could be considered not to be a reasonable response. The ACMA must then give a copy of its determination to the service provider.

256. Subsection 187G(6) will set out what the CAC must do in relation to implementation plans amended by the service provider in accordance with a determination by the ACMA and given to the CAC. While no particular timeframe is specified in the subsection for a service provider to provide an amended plan to the CAC, the service provider should provide the amended plan within a reasonable period of time. (A guide for a reasonable period of time would be 30 days). The CAC must then either approve the amended plan or refuse to approve the plan. In either case, the CAC must notify the service provider accordingly.

257. While no specific factors are set down in section 187G, in making decisions under proposed section 187G, the CAC and the ACMA should generally take into account the list of factors in proposed subsection 187F(2).

258. Subsection 187G(7) will provide that a determination by the ACMA under subsection 187G(5) is not a legislative instrument. Subsection 187G(7) will be included to assist readers, as a determination made by the ACMA under section 187G(5) is not a legislative instrument within the meaning of section 5 of the *Legislative Instruments Act 2003*.

New section 187H—When data retention implementation plans are in force

259. Section 187H will set out when data retention implementation plans are in force.

260. Paragraph 187H(1)(a) will provide that a data retention implementation plan for a telecommunications service operated by a service provider commences when the CAC notifies the service provider of the CAC's approval of the plan (which can be either the service provider's original plan or an amended plan).

261. Paragraph 187H(1)(b) will also set out that an implementation plan ceases to be in force in relation to a service operated, in the following circumstances:

i. For telecommunications services that the service provider was already operating when Part 5-1A of the TIA Act commenced, the plan ceases to be in force 18 months after commencement of Part 5-1A of the TIA Act.
ii. For telecommunications services that the service provider was not already operating when Part 5-1A of the TIA Act commenced, the plan ceases to be in force 18 months after when the service provider started operating the service.

262. Subsection 187H(2) will define the term ‘implementation phase’ for the purposes of Part 1 of Schedule 1 of the TIA Act as being the end of the period of 18 months starting on the commencement of Part 5-1A.

New section 187J—Amending data retention implementation plans

263. Section 187J will set out when a data retention implementation plan can be amended. The purpose of this provision is to ensure that, once approved, a data retention implementation plan may only be varied with the consent of both the service provider and the CAC. This limitation is intended to provide regulatory certainty for service providers, and to ensure that law enforcement and national security interests are considered in relation to any variation.

264. Subsection 187J(2) will provide that the rules for the CAC to approve implementation plans under section 187F and section 187H also apply to applications for amendments of plans by a service provider under paragraph 187J(1)(a), as if the amendment application had been an application in relation to an original plan under section 187E. This means that the CAC will be required to assess proposed amendments of implementation plans under section 187J in the same way as the CAC would assess applications in relation to original plan applications made under section 187E.

265. Paragraph 187J(3)(a) will provide that an amendment to a data retention implementation plan comes into force when the CAC notifies the service provider of the approval of an amendment, or when the service provider agrees to an amendment requested by the CAC. Paragraph 187J(3)(b) will provide that an amendment to a data retention plan cannot reduce or extend the period for which the implementation plan is in force (although an amended plan could specify that full compliance will be achieved prior to the end of period for which the plan is in force).

Division 3 of Part 5-1A—Exemptions

New section 187K—The Communications Access Co-ordinator may grant exemptions or variations

266. New section 187K will provide that the CAC may exempt a service provider from the mandatory data retention obligations imposed on the service provider under new Part 5-1A of the TIA Act, or vary the obligations that the service provider is subject to. The CAC may grant this exemption or variation on his or her own volition or on application by a service provider.

267. This exemption and variation scheme is intended to permit exemptions or variations to be granted in a range of circumstances, including where imposing data retention obligations for a particular relevant service would be of limited utility for law enforcement and national security purposes.

268. The scheme provided by this section is modelled on existing sections 192 and 193 of the TIA Act, which provide that the CAC or the ACMA may grant exemptions in relation to the interception capability obligations of service providers.

269. Subsection 187K(1) provides that the CAC may make a determination in relation to a specified service provider that:

- removes or varies any or all of the mandatory data obligations
- removes or varies any or all of the mandatory data obligations imposed on the service provider under Part 5-1A for a particular kind of relevant service, or
- reduces the data retention period, either generally or in relation to data that relates to a particular kind of relevant service.

270. A variation must not, however, impose obligations that would exceed the obligations to which a service provider would otherwise be subject to under sections 187A and 187C.

271. The decision of the CAC may be expressed broadly. In making a determination, the CAC may specify service providers in any way, for example by reference to a class of service providers, and will not have to refer specifically to individual service providers. For example, the CAC may specify that any service provider that provides Internet Protocol television (IPTV) services is not required to retain any data in relation to its IPTV service. Similarly, an exemption or variation may be expressed to apply to a class of obligations.

272. Subsection 187K(1) will ensure that determinations can be properly nuanced by vesting the CAC with the ability to elaborate, either to particular service providers or generally, how the data retention obligations introduced by Part 5-1A should apply to particular technologies. For example, a determination could exempt the retention of specific information relating to satellite or mobile internet services. Those services create different types of data, therefore it is appropriate to have a method of providing greater certainty to service providers about how high-level obligations apply to diverse technologies.

273. The data retention obligations under proposed Part 5-1A may cover services that are of limited or no relevance to law enforcement or national security. These could include services relating to IPTV, content on demand, the leasing of dark fibre and machine-to-machine communications. Subsection 187K(1) recognises that, in certain instances, a service provider may not achieve complete technical compliance in relation to a particular service or some aspect of that service, or that the non-compliance has limited implications for law enforcement or national security agencies.

274. The decision of the CAC to grant an exemption or variation is not reviewable under the *Administrative Decisions (Judicial Review) Act 1977* (the ADJR Act) as decisions under the TIA Act are not decisions to which the ADJR Act applies (see paragraph (d) of Schedule 1 to the ADJR Act). The exclusion of these decisions from the ADJR Act does not prevent decisions made under the TIA Act from being judicially reviewable under paragraph 75(v) of the Constitution and section 39B of the *Judiciary Act 1901* (Cth).

275. Subsection 187K(2) will provide that the CAC's decision must be in writing.

276. Subsection 187K(3) will provide that the CAC's decision may be unconditional, or subject to such conditions as specified in the exemption or variation. Such conditions may include limits on the time for which the exemption or variation applies, limits on the numbers of customers or the geographic scope of a particular type of service, or requirements for ongoing consultations with agencies.

277. Subsection 187K(4) will provide that a decision made by the CAC under subsection 187K(1) is not a legislative instrument. Subsection 187K(4) has been included to assist readers, as the instrument is not a legislative instrument within the meaning of section 5 of the *Legislative Instruments Act 2003.*

278. Paragraph 187K(5)(a) will provide that where a service provider applies in writing for a particular decision, the CAC must give a copy of the application to affected enforcement agencies or security agencies and may give a copy to the ACMA. Where the requested exemption has an impact on the investigative capabilities or regulatory functions of an agency, it is appropriate that the CAC consults with that agency.

279. Paragraph 187K(5)(b) will provide that if the CAC does not respond to a service provider's application within 60 days, the decision requested by the service provider is deemed to have been granted to that service provider. This provision is intended to ensure that the CAC resolves applications in a timely manner and provides certainty for service providers as to their legal obligations under the TIA Act at any given time.

280. Subsection 187K(6) will provide that the deemed decision under paragraph 187K(5)(b) has effect only until the CAC makes and communicates to the service provider a decision on the application. This will ensure that the deemed exemption is only temporary.

281. Subsection 187K(7) will require that, in granting an exemption or variation, the CAC must take into account the interests of law enforcement and national security, which can include the relevance to law enforcement or national security of the services for which an exemption or variation is being sought.

282. The CAC must also take into account the objects of the *Telecommunications Act 1997*,[14] the main object of which is to provide a regulatory framework that promotes:

- the long-term interests of users of telecommunications services,
- the efficiency and international competitiveness of the Australian telecommunications industry, and
- the availability of accessible and affordable carriage services that enhance the welfare of Australians.

283. The CAC must also take into account the service provider's history of compliance with Part 5-1A of the TIA Act, the service provider's costs, or anticipated costs, of complying with data retention obligations under Part 5-1A, and any alternative data retention arrangements that the service provider has identified. Such alternative data retention arrangements could be formalised as part of an exemption or variation granted by the CAC. Service providers are in a unique position to draw to the CAC's attention specific cost implications, and to suggest alternative compliance arrangements in support of any exemption application.

[14] See section 3 of the *Telecommunications Act 1997*.

284. Subsection 187K(8) will enable the CAC to take into account any other relevant matter when deciding whether or not to grant an exemption or variation, which might include relevant technological or industry factors such as:

- the size, market share and national security and law enforcement risk profile of the service provider,
- the degree to which an exemption would effectively mitigate costs and minimise impacts on the service provider's cash flow, and
- the pre-existing business plans of the service provider.

285. Pursuant to section 33(3) of the *Acts Interpretation Act 1901*, the power to make or grant an instrument of administrative character, such as an exemption or variation under subsection 187K, is to be taken as including a power to repeal, rescind, revoke, amend or vary any such instrument. This power is to be exercised in the same manner and subject to the same conditions (if any) that applied to the making or granting of the instrument.

286. The CAC may seek to exercise the power to repeal or revoke an exemption or variation in a range of circumstances, including where an exemption (that has been granted on the expectation that it will remain confidential) becomes known publicly, to a class of persons, or to a specific individual in circumstances where that disclosure would have a detrimental impact on the interests of law enforcement and national security.

Division 4—Miscellaneous

New section 187L—Confidentiality of applications for exemptions etc

287. Subsection 187L(1) will place an obligation on the CAC to treat a service provider's application for a data retention implementation plan or an exemption from the data retention obligations as confidential, and must not disclose the service provider's application, without the written permission of the service provider. This prohibition does not apply to disclosure to the Australian Communications and Media Authority (the ACMA), an enforcement agency or a security authority. It is appropriate that the CAC is able to consult with affected agencies and the ACMA about such applications.15

288. Subsection 187L(2) will provide that where a copy of an application is disclosed to the ACMA, an enforcement agency or a security authority, that body must treat the copy as confidential, and may not disclose it to any other person or body without the written permission of the carrier. This subsection is modelled on section 202 of the TIA Act.

289. A service provider's application for an exemption will include details about specific business processes, such as technical network infrastructure specifications which would be commercial-in-confidence. The obligation on the CAC, as well as any agencies that the application was disclosed to, to treat such applications as confidential reflects the sensitivity of the information contained in such applications, from both a commercial and national security perspective.

290. Section 187L will not require service providers to keep applications, approved implementation plans or exemptions confidential. However, revealing the existence of the fact that a service provider is not subject to data retention obligations under section 187A and 187C in relation to a particular relevant service may give rise to new or increased law enforcement and national security risks that may, in all of the circumstances, justify the CAC revoking an exemption.

New section 187M—Pecuniary penalties and infringement notices

291. Section 187E will provide that the data retention obligations set out in proposed subsection 187A(1) and the obligations under data retention implementation plans under proposed paragraph 187D(a) will be civil penalty provisions for the purposes of the Telecommunications Act. The effect of this will be to clarify that the new telecommunications data retention regime and data retention implementation plans are enforceable under the applicable enforcement mechanisms set out in the Telecommunications Act.

292. The Telecommunications Act already requires compliance with carrier licence conditions (for carriers) or service provider rules (for carriage service providers), which require, amongst other things, compliance with Chapter 5 of the TIA Act.

293. Enforcement options available in the Telecommunications Act for non-compliance with the data retention regime or a data retention implementation plan will include things such as remedial directions, formal warnings and pecuniary penalties.

[15] See also note on new paragraph 187K(5)(a) at paragraph [112] of this Explanatory Memorandum.

294. Infringement notices are notices issued to carriers/carriage service providers (C/CSPs) by the ACMA in relation to contravention of civil penalty provisions of the Telecommunications Act (which can include for these purposes the TIA Act). The notices are designed as a more efficient means of dealing with certain penalty provisions as an alternative to instituting court proceedings for the recovery of a pecuniary penalty.

295. Subsection 572E(1) of the Telecommunications Act provides that ACMA can issue an infringement notice if a C/CSP has contravened a civil penalty provision. Proposed section 187M defines the data retention obligations in subsection 187A(1) and the data retention implementation obligations in paragraph 187D(a) as civil penalty provisions. This means the ACMA will be able to issue infringement notices in relation to contraventions of these provisions.

296. Subsections 572E(6) to (9) of the Telecommunications Act refer to a process for declaring contraventions of certain carrier licence conditions and service provider rules under the Telecommunications Act before the ACMA can issue infringement notices in relation to those matters. It will not be necessary for the ACMA to declare contraventions of subsection 187A(1) or paragraph 187D(a) of the TIA Act to be listed infringement notice provisions before ACMA can issue infringement notices in relation to these matters. This is because proposed section 187M of the TIA Act will declare these provisions to be civil penalty provisions in their own right.

New section 187N—Review of operation of Part

297. Section 187N will provide that the PJCIS must review the operation of new Part 5-1A of the TIA Act as soon as practicable after the third anniversary of the end of the implementation phase for data retention obligations. Subsection 187N(2) will require the PJCIS to give the Minister a written report of the review. This requirement is not intended to prevent the Chair of the PJCIS from tabling that report in Parliament.

298. Section 187N will give effect to the relevant part of Recommendation 43 of the 2013 PJCIS report, that the effectiveness of any mandatory data retention regime be reviewed by the PJCIS three years after its commencement.

299. Section 187N will also ensure that, after the data retention regime has been in operation for a sufficient period of time, a review is conducted to ensure the regime is operating appropriately.

300. The requirement under new subsection 187N(2) for the Committee to provide the Minister with a copy of the report is not intended to preclude the Chair of the Committee from tabling that report in Parliament.

New section 187P—Annual reports

301. Section 186 of the TIA Act lists the information enforcement agencies must provide to the Minister about data authorisations. This information is included in the Annual Report about the use of powers under the TIA Act prepared under Part 2-8 of the TIA Act and tabled by the Minister in each House of the Parliament. Subsection 187P(1) will provide that the Minister must prepare a written report on the operation of Part 5-1A (regarding data retention obligations) for each financial year. Subsection 187P(2) will require that the report be included in the Annual Report under subsection 186(2) of the TIA Act which enables the

Minister to include any information in the Annual Report that the Minister considers appropriate.

302. Subsection 187P(3) will provide that the report under subsection 187P(1) must not be made in a manner that would be likely to identify a person.

303. Section 187P will implement the relevant part of Recommendation 43 of the 2013 PJCIS report that if data retention is implemented, there should be an annual report to Parliament on the operation of the scheme. The requirement to report on the regime is consistent with the general reporting and accountability obligations already contained in the TIA Act.

PART 2—OTHER AMENDMENTS

Telecommunications Act 1997

Item 2—Section 7 (at the end of the definition of *civil penalty provision)*

304. This item will amend section 7 of the Telecommunications Act to clarify that a provision of the TIA Act that is declared to be a civil penalty provision is a civil penalty provision for the purposes of the TIA Act. Proposed section 187M of the TIA Act provides that the data retention obligations set out in new subsection 187A(1) and data retention implementation plan obligations in new paragraph 187D(a) are civil penalty provisions.

Item 3—Subsection 105(5A)

305. This item will amend section 105 of the Telecommunications Act, which sets out the matters on which ACMA must monitor and report in its annual reports. This clause will repeal and substitute subsection 105(5A) of the Telecommunications Act to provide that ACMA must monitor and report each financial year to the Minister on:

- The operation of Part 14 of the Telecommunications Act (which governs the assistance that carriers, carriage service providers and carriage service intermediaries must provide in relation to national security and law enforcement matters) and the costs of compliance with Part 14, and
- The costs of compliance with data retention capability obligations set out in Part 5-1A of the TIA Act.

306. Proposed paragraph 105(5A)(a) of the Telecommunications Act is only intended to re-enact the repealed subsection 105(5A) of the Telecommunications Act and no change in meaning is intended. However, new paragraph 105(5A)(a) will delete an obsolete reference from subsection 105(5A) of the Telecommunications Act to Part 15 of that Act, which was repealed by the *Telecommunications (Interception and Access) Amendment Act 2007*.

307. Proposed paragraph 105(5A)(b) of the Telecommunications Act will require ACMA to monitor and report on the costs of data retention. The purpose of paragraph 105(5A)(b) will be to provide public accountability about the costs to the telecommunications industry of implementing data retention obligations by providing that the ACMA must monitor and report on these matters.

Item 4– Subsection 314(8)

308. Section 314 of the Telecommunications Act concerns the terms and conditions on which carriers, carriage service providers and carriage service intermediaries must provide reasonably necessary assistance in relation to national security and law enforcement matters.

309. Subsection 314(8) of the Telecommunications Act clarifies that certain obligations set out in the TIA Act are not included within the provisions of section 314 of the Telecommunications Act. This item will amend subsection 314(8) of the Telecommunications Act to provide that section 314 of the Telecommunications Act does not apply in relation to data retention capability obligations set out in Part 5-1A of the TIA Act.

Telecommunications (Interception and Access) Act 1979

Item 5—Subsection 5(1)

Implementation phase

310. This item will insert a definition of 'implementation phase' into subsection 5(1) of the TIA Act. It will take on the meaning set down in subsection 187H(2). Section 187H relates to when data retention implementation plans are in force. The term 'implementation phase' is defined to mean, in relation to Part 5-1A of the TIA Act, 'the end of the period of 18 months starting on the commencement' of Part 5-1A of the TIA Act.

Service provider

311. This item will also insert a definition of 'service provider' into subsection 5(1) of the TIA Act, which will be the meaning of that term in proposed subsection 187A(1).

Item 6—At the end of subsection 6R(3)

312. This item will amend subsection 6R(3) of the TIA Act to provide that an act done by the CAC is done on behalf of all enforcement agencies, in addition to being done on behalf of interception agencies.

313. The purpose of this provision is to support the decisions of the CAC in relation to exemptions from the new mandatory data retention regime made in relation to enforcement agencies that are not also interception agencies.

PART 3—APPLICATION PROVISIONS

Item 7—Existing information and documents

314. Subitem (1) will provide that the requirements on service providers to keep data contained in Schedule 1 apply in relation to information and documents already being kept by service providers immediately before the commencement of this item, where the service provider had not already kept the information or documents for longer than the retention period specified by new section 187C.

315. This will ensure that any existing information and documents that have been in existence for less than two years will be retained by service providers, and will remain available for law enforcement and national security purposes.

316. These obligations may be modified under a data retention implementation plan or an exemption approved under Part 5-1A.

317. Subitem (2) is intended to provide clarification that the requirement in subitem (1) to retain existing information and documents will not require a service provider to create any information or document that was not already created by the operation of a carriage service before the commencement of this item.

318. The data retention requirements contained in new Part 5-1A as inserted by Item 1 of Schedule 1 do not have retrospective application.

Item 8—Reducing the period for keeping information or documents

319. This item will commence on Royal Assent and requires that service providers must not reduce the length of time for which they retain information or documents that will be subject to data retention obligations under Part 5-1A in the period between Royal Assent and the commencement of Part 5-1A.

320. The purpose of this item is to prevent any further degradation of industry retention practices prior to the commencement of Part 5-1A.

321. This item will interact with the implementation planning and exemption frameworks. An implementation plan approved under new section 187F, or an exemption granted under new section 187K, may modify the period for which a service provider will, after the commencement of Part 5-1A, be required to keep or cause to be kept information or documents under Part 5-1A. As such, if a service provider has an implementation plan approved or is granted an exemption prior to the commencement of Part 5-1A, the provider will be permitted to keep the information or documents covered by that plan or exemption for the period specified in that plan or exemption, even if that period is shorter than the period for which the service provider kept that information or those documents at Royal Assent.

322. This item will be taken to be a civil penalty provision for the purposes of the Telecommunications Act.

Item 9—Applications made before commencement of Part 5-1A

323. Subitem 9(1) will provide that at any time after this legislation receives the Royal Assent a service provider may apply to the Communications Access Co-ordinator (the CAC) for either or both of the following:

a. (i) approval of a data retention implementation plan

(ii) an amendment of a data retention implementation plan, and

b. a decision to exempt the service provider from any or all of the obligations under new subsection 187K(1).

324. This will enable service providers to seek approval of plans and to facilitate a decision by the CAC on the request before the commencement of the data retention obligations.

325. Subitem 9(2) will provide that paragraph (1)(a) of this item (application for the approval of a data retention implementation plan after the Royal Assent) does not apply unless the application would, if it had been made after the commencement of new Part 5-1A, have complied with the requirements for applying for the approval of data retention implementation plans under new section 187E.

326. The effect of this subitem is to require that applications by a service provider made prior to the commencement of the main data retention amendments for the approval of a data retention implementation plan must still comply with the requirements for such an application under new section 187E.

327. Subitem 9(3) will provide that applications for the approval of a data retention implementation plan made under paragraph 9(1)(a) will be taken to be an application under new section 187E for the purposes of subsection 187E(4).

Item 10—Decisions made before commencement of Part 5-1A

328. Subitem 10(1) will provide that the power of the CAC to make decisions under new sections 187F (approval of data retention implementation plans), 187G (consultation with interception agencies and the ACMA), 187J (amending data retention implementation plans) and 187K (exemptions) is taken, for the purposes of section 4 of the *Acts Interpretation Act 1901* (AIA), to be a power to make an instrument of an administrative character.

329. Section 4 of the AIA allows for the exercise of powers of an administrative character conferred by an Act before the commencement of that Act.

330. The ability of the CAC to make these decisions before the commencement of new Part 5-1A (as inserted by Item 1 of Schedule 1 of this legislation) will ensure that the data retention scheme will be fully effective upon the commencement of the main amendments.

331. Subitem 10(2) is a transitional application provision. It will provide that new subsection 187F(3) applies, in relation to applications for the approval of data retention implementation plans made before the commencement of Part 5-1A, as if references in that subsection to 60 days were references to the number of days provided for in subitem (4) of this item.

332. New subsection 187F(3) will provide that a service provider's application to the CAC for the approval of a data retention implementation plan is deemed to have been granted if the CAC does not make a decision within 60 days.

333. Subitem 10(3) is a transitional application provision. It will provide that new paragraph 187K(5)(b) applies, in relation to applications for exemptions made before the commencement of Part 5-1A, as if references in that subsection to 60 days were references to the number of days provided for in subitem (4).

334. New subsection 187K(5) will provide that a service provider's application to the CAC for an exemption from the data retention obligations under new section 187A is deemed to have been granted if the CAC does not make a decision within 60 days.

335. Subitem 10(4) provides that for the purposes of subitems 10(2) and (3), the number of days is the period between the day the application was made and the day immediately before Part 5-1A commences; and 60 days, whichever is greater.

336. Subitems 10(2) and (3) will have the effect of providing the CAC with at least 60 days to consider applications before an approval is deemed. This time period will ensure that the CAC will have enough time to properly consider any applications received prior to the commencement of Part 5-1A.

Item 11—Keeping information or documents before commencement of Part 5-1A

337. This item will provide that a service provider may keep or cause to be kept the information or documents the service provider is required to keep or cause to be kept under the data retention obligations contained in new Part 5-1A as inserted by Item 1 of Schedule 1, before the commencement of those data retention obligations.

338. Australian Privacy Principles 3.2 and 11.2 prohibit entities from collecting and retaining data that is not reasonably necessary for its functions or activities in the absence of a legislative obligation (which will not exist until the data retention obligations commence) to do so.

339. However, it may be more commercially efficient for a carrier to commence retaining data at some point prior to the commencement of the data retention obligations. For example, if a carrier designs and builds a new data retention system, it may wish to shut down its existing system and transition to the new system prior to the commencement date to save on capital and operating costs.

340. This provision will ensure that service providers are not in breach of their obligations under the *Privacy Act 1988* should they retain relevant data before the commencement of the data retention requirements.

SCHEDULE 2— RESTRICTING ACCESS TO STORED COMMUNICATIONS AND TELECOMMUNICATIONS DATA

Overview of measures

341. This Schedule will amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to limit the types of agencies that can apply for stored communications warrants under Part 3-3 of Chapter 3 of the TIA Act and the types of authorities and bodies that can authorise the disclosure of telecommunications data under Division 4, Part 4-1 of Chapter 4 of the TIA Act.

342. These amendments recognise the widespread community acceptance and use of stored communications (including text messages and emails) and the greater privacy sensitivity of these communications, which reveal content and the substance of a person's discussions with others, compared to telecommunications data. Currently, authorities and bodies that are an 'enforcement agency' can apply to an independent issuing authority (appointed under section 6DB of the TIA Act) for a stored communications warrant to investigate a 'serious contravention' of the law. While this requirement limits the availability of stored communications warrants to enforcement agencies that investigate offences with at least a three year imprisonment penalty or a fine of at least 900 penalty units, this Schedule will further reduce the availability of stored communications warrants by limiting access to stored communications to agencies that are criminal law-enforcement agencies.

343. Currently, access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits enforcement agencies to authorise telecommunications carriers to disclose telecommunications data where that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue. An 'enforcement agency' is broadly defined to include all interception agencies as well as a body whose functions include administering a law imposing a pecuniary penalty or administering a law relating to the protection of the public revenue. In practice, the range of agencies that are enforcement agencies and who can authorise the disclosure of telecommunications data is broad and includes local government councils and Commonwealth and State Departments and Agencies. In 2012-13, approximately 80 enforcement agencies made historic data authorisations.[16]

344. Schedule 2 will amend the existing definition of 'enforcement agency' to limit access to telecommunications data to criminal law-enforcement agencies and authorities or bodies that have been declared by the Minister to be an 'enforcement agency'. These amendments are consistent with the recommendation of the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) in the 2013 *Report of the inquiry into potential reforms of Australia's national security legislation* (Recommendation 5),[17] that the number of agencies able to access telecommunications data be reduced.

345. These amendments are also consistent with Australia's international legal obligations under the *Convention on Cybercrime.* Article 14(2) of the Cybercrime Convention[18] requires

[16] Australian Government Attorney-General's Department (2013), *Telecommunications (Interception and Access) Act 1979 Annual Report 2012-13*, 47-51.
[17] Available at <http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm>.
[18] Opened for signature 23 November 2001, ETS 185 (entered into force 1 July 2004).

parties to ensure that telecommunications data (and other evidence in electronic form, other than the content of communications and prospective or future telecommunications data) is available for the investigation of any criminal offence.[19] Schedule 2 complies with this obligation by ensuring that telecommunications data is available to agencies with a demonstrated need to access data.

346. The data access arrangements contained in Schedule 2 are subject to new oversight and accountability requirements detailed in Schedule 3 of the Bill. Together, the Schedules introduce a new data access framework that better protects privacy while ensuring that data is available to investigate criminal offences and other activities that threaten community safety and security.

347. Part 1 of this Schedule contains the main amendments to Chapters 3 and 4. These provisions will restrict access to stored communications to criminal law enforcement agencies, and will amend the definition of 'criminal law enforcement agency' and 'enforcement agency'.

348. Part 2 of this Schedule contains other amendments that are consequential to the amendments contained in Part 1.

349. Part 3 of this Schedule provides for how the amendments contained in Schedule 2 apply upon their commencement.

PART 1—MAIN AMENDMENTS

Telecommunications (Interception and Access) Act 1979

Item 1—Subparagraphs 107J(1)(a)(i) and (ii)

350. Subparagraph 107J(1)(a)(i) of the TIA Act enables any enforcement agency to issue a historic domestic preservation notice to a carrier to preserve specified stored communications held by a carrier on the day the notice is received. Subparagraph 107J(1)(a)(ii) allows enforcement agencies that are also interception agencies to issue ongoing preservation notices. Ongoing notices require carriers to keep relevant stored communications held by the carrier for up to 30 days from receipt of the notice. The term 'interception agency' is defined in section 5 of the TIA Act and is limited to agencies such as the Australian Federal Police and State Police Forces eligible to apply under Part 2-5 of the TIA Act for an interception warrant.

351. Item 1 will remove the references to an 'enforcement agency' in subsection 107(J)(1) of the TIA Act and substitute the new definition of a 'criminal law-enforcement agency' in section 110A of the Act. Amending the definition will strengthen privacy protections in relation to stored communications by limiting the availability of historic domestic preservation notices to those agencies who can apply for stored communications warrants under the TIA Act as amended by this Schedule. Ongoing domestic preservation notices will continue to be limited to interception agencies.

[19] See also Council of Europe, Explanatory Report to the Convention on Cybercrime, paragraph 141.

Item 2—Subsection 110(1)

352. Subsection 110(1) of the TIA Act provides that an enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.

353. Item 2 will remove the reference to an 'enforcement agency' in subsection 110(1) of the Act and substitute the new definition of a 'criminal law-enforcement agency' in section 110A of the Act.

354. Amending the definition will reduce the number of agencies that can apply for stored communications warrants from all enforcement agencies that investigate serious contraventions to those authorities and bodies that are recognised under new section 110A of the Act as being criminal law-enforcement agencies.

Item 3—After section 110

New section 110A – meaning of *criminal law-enforcement agency*

355. Currently, criminal law-enforcement agencies can issue historic domestic preservation notices, and access stored communications and prospective telecommunications data. Agencies that fall within the broader definition of 'enforcement agency' are also able to issue historic domestic preservation notices and apply for stored communications warrants.

356. New section 110A will insert a new definition of 'criminal law-enforcement agency' after section 110 of the TIA Act. The new definition will remove the ability of enforcement agencies that are not also criminal law-enforcement agencies to issue historic domestic preservation notices under subsection 107J(1) and to apply for stored communications warrants under section 110 of the Act. These amendments recognise that while governments at all levels have charged a range of authorities and bodies with responsibility for investigating or enforcing offences punishable by significant prison terms (at least a three year term) access to stored communications should be limited to agencies with a demonstrated investigative need and practices to safeguard the use and disclosure of information obtained under a stored communications warrant.

Subsection 110A(1) – meaning of criminal law-enforcement agency

357. Subsection 110A(1) will provide that the following agencies, authorities and bodies are 'criminal law-enforcement agencies':

(a) the Australian Federal Police
(b) a Police Force of a State
(c) the Australian Commission for Law Enforcement Integrity
(d) the Australian Crime Commission
(e) the Australian Customs and Border Protection Service
(f) the Crime Commission
(g) the Independent Commission Against Corruption
(h) the Police Integrity Commission
(i) the Independent Broad-based Anti-corruption Commission
(j) the Crime and Corruption Commission of Queensland
(k) the Corruption and Crime Commission

(l) the Independent Commissioner Against Corruption, and
(m) subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.

358. New section 110A will include all the interception agencies listed in the current definition of criminal law-enforcement agency in section 5(1) of the TIA Act. The Australian Customs and Border Protection Service will also be included as it is prescribed by the *Telecommunications (Interception and Access) Regulations 1987* to be a criminal law-enforcement agency for the purposes of paragraph (k) of the definition of 'enforcement agency' in subsection 5(1) of the TIA Act.

359. New paragraph 110A(1)(m) will allow the Minister to declare authorities or bodies to be criminal law-enforcement agencies to accommodate the creation of any new agencies or any changes in agency functions over time.

Subsections 110A(2) to (6) – Declaration of an authority or body as a criminal law-enforcement agency

360. New subsections 110A(2) to (9) will allow the Minister to declare authorities or bodies to be 'criminal law-enforcement agencies' for the purposes of paragraph 110A(1)(m). This power will replace paragraph (k) in the definition of enforcement agency in section 5(1) of the TIA Act that allows the Governor-General to make regulations prescribing an agency to be an enforcement agency. Agencies that are prescribed under paragraph (k) are also criminal law-enforcement agencies for the purposes of the TIA Act.

361. Under new subsection 110A(2), the head of an authority or body will be able to ask the Minister to declare the authority or body to be a criminal law-enforcement agency. New subsection 110A(3) will also allow the Minister to make a declaration without an application.

362. Before making a declaration, the Minister must consider the factors listed in paragraphs (a)-(f) of new subsection 110A(4). The current regulation making power in relation to paragraph (k) of the definition of enforcement agency does not prescribe any factors that must be considered in making a decision whether or not to prescribe an agency. New subsection 110A(4) will ensure that authorities and bodies provide consistent and detailed information about their functions and privacy practices necessary to make an informed decision about an agency's need to access stored communications and the appropriateness of that agency having such information.

363. New subsection 110A(5) means that the Minister will be able to consult with any persons or bodies the Minister considers should be consulted with before making a declaration under subsection 110A(4). The Minister can consult with the Commonwealth Privacy Commissioner and the Commonwealth Ombudsman but is not limited to consulting with those bodies.

364. New subsection 110A(6), when read with new subsection 110A(7), means that authorities and bodies may only be granted the status of a criminal law-enforcement agency or enforcement agency for certain powers available under Chapter 3 or Chapter 4 of the TIA Act. Authorities may investigate a range of offences only some of which are serious contraventions (under section 5E of the TIA Act serious contraventions are limited to

offences punishable by a period, or a maximum period, of at least three years' imprisonment or an equivalent fine or pecuniary penalty). In these circumstances the interaction of these two subsections means the Minister could limit an authority's status as a criminal law enforcement agency to the offences with a three year or more imprisonment term.

365. New subsection 110A(3) will also enable the Minister to declare certain persons specified in the declaration to be 'officers' of the criminal law-enforcement agency. Under the TIA Act, officers, as defined in subsection 5(1) of the Act, have various roles and responsibilities. For example, under section 110 of the TIA Act, applications for stored communications warrants can be made on an agency's behalf by officers holding a management position in that agency. Enabling persons to be declared as officers of a particular criminal law enforcement agency will facilitate the effective operation of the TIA Act in relation to that agency.

366. Decisions about declarations are not subject to review under the *Administrative Decisions Judicial Review Act 1977* (the ADJR Act) as decisions under the TIA Act are not decisions to which the ADJR Act applies (see paragraph (d) of Schedule 1 to the ADJR Act). The exclusion of these decisions from the ADJR Act does not prevent decisions made under the TIA Act from being judicially reviewed under paragraph 75(v) of the Constitution. Declarations under subsection 110A(3) are also subject to parliamentary review as they are legislative instruments under the *Legislative Instruments Act 2003* and can be disallowed under Part 5 of that Act.

367. New subsection 110A(8) will enable the Minster to revoke a declaration made under subsection (3) if the Minister is no longer satisfied that the circumstances justify the declaration remaining in force. This provision will address a shortfall in the current Act whereby agencies that meet the definition of a criminal law-enforcement agency retain that status even if their functions change. New subsection 110A(8) will ensure that only agencies with a demonstrated need for stored communications will be able to obtain this information.

368. Under new subsection 110A(9) the revocation of a declaration will not affect the validity of:

- a domestic preservation notice given by the authority or body
- a stored communications warrant issued to the authority or body that was in force immediately before the revocation took effect, or
- an authorisation made by an authorised officer of the authority or body under Division 4 of Part 4-1.

369. This will allow authorities and bodies to rely on notices and authorisations already issued or warrants already obtained for the duration of their independent validity period and protect carriers who act on a notice, authorisation or a stored communications warrant before becoming aware of the revocation.

Item 4—Before section 177

New section 176A – meaning of *enforcement agency*

370. Item 4 will insert new section 176A before section 177 of the TIA Act.

371. New section 176A will replace the current definition of 'enforcement agency' in subsection 5(1) of the TIA Act with a definition that limits the authorities and bodies that can access telecommunications data to criminal law-enforcement agencies and authorities and bodies declared under section 176A to be an enforcement agency.

372. Currently the definition of 'enforcement agency' in section 5(1) of the TIA Act provides that the following agencies are enforcement agencies:

(a) the Australian Federal Police
(b) a Police Force of a State
(c) the Australian Commission for Law Enforcement Integrity
(d) the Australian Crime Commission
(e) the Crime Commission
(f) the Independent Commission Against Corruption
(g) the Police Integrity Commission
(h) the Independent Broad-based Anti-corruption Commission
(i) the Crime and Misconduct Commission
(j) the Corruption and Crime Commission
(ja) the Independent Commissioner Against Corruption
(k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph
(l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management - Police
(m) the CrimTrac Agency
(n) any body whose functions include:
    (i) administering a law imposing a pecuniary penalty; or
    (ii) administering a law relating to the protection of the public revenue.

373. The reference to 'criminal law-enforcement agency' in new paragraph 176A(a) will replace the agencies listed at paragraphs (a) to (k) in the current definition (see Item 3 above).

374. Current paragraph (l) of the definition of 'enforcement agency' is an open-ended description and will be omitted from new paragraph 176A. Deleting this reference will ensure that only agencies specifically listed in the section, or declared to be enforcement agencies following consideration of the factors listed in paragraph 176A(4), can access telecommunications data.

375. Current paragraph (m), which refers to the CrimTrac Agency, will also be deleted from the new definition. CrimTrac develops and maintains national police information sharing services between Australian law enforcement agencies, particularly by delivering national database systems such as the National Child Sex Offender Register, the National Automated Fingerprint Identification System and the National Criminal Investigation DNA Database. CrimTrac does not however, enforce laws by investigating and prosecuting specific instances of wrongdoing (whether in a primary or supporting role).

376. Current paragraph (n) will be removed from the new definition. Paragraph (n) is broad and increases the possibility that authorities and bodies that do not have a compelling current

need to access telecommunications data may be able to authorise the disclosure of this information. The definition as unamended by this Bill encompasses a wide range of Commonwealth, State, Territory and local government agencies as well as bodies such as the Royal Society for the Prevention of Cruelty to Animals that have law enforcement roles under State legislation. Many of these bodies are responsible for investigating serious activities and behaviours. For example, under Queensland's Animal Care and Protection Act 2001, the offence of animal cruelty has a maximum penalty of 2,000 penalty units or 3 years imprisonment.

377. While the existing arrangements limit who within an authority or body can access telecommunications data and for what purposes, the scope of current paragraph (n) means that telecommunications data could potentially be available to a large number of agencies as the TIA Act does not have a clear mechanism for determining which authorities and bodies fall within the definition of an 'enforcement agency'. New section 176A will rectify this concern by introducing a power at subsection 176A(3) for the Minister to declare a specific authority or body to be an enforcement agency for the purposes of the TIA Act.

Subsections 176A(2) to (7) – Declaration of an authority or body as an enforcement agency

378. Subsections 176A(2) to (7) will set out the process to be used by the Minister in considering whether to declare an authority or body to be an enforcement agency.

379. Under proposed subsection 176A(2) the head of an authority or body will be able to request that the Minister declare the authority or body to be an enforcement agency. New subsection 176A(3) will allow the Minister to make a declaration without an application.

380. Before making a declaration, the Minister must consider the factors listed in paragraphs (a)-(f) of new subsection 176A(4). These factors include considering whether an authority or body complies with the Australian Privacy Principles or a comparable scheme or proposes to comply with a scheme providing a similar level of privacy protection. New subsection 176A(4) will ensure that authorities and bodies provide consistent and detailed information about their functions and privacy practices necessary to make an informed decision about an authority's or body's need to access telecommunications data and the appropriateness of that authority or body having such information.

381. New subsection 176A(5) means that the Minster will be able to consult with any persons or bodies the Minister considers should be consulted before making a declaration under subsection 176A(4). The Minister can consult with the Commonwealth Privacy Commissioner and the Ombudsman but is not limited to consulting with those bodies.

382. New subsection 176A(6) when read with new subsection 176A(7) means that an authority or body may only be granted the status of an enforcement agency for certain powers available under Chapter 4 of the TIA Act. For instance, an authority's functions may include administering legislation that imposes pecuniary penalties of a minor degree as well as offences with significant penalties and terms of imprisonment. In these circumstances the interaction of these two subsections means the Minister could limit an authority's ability to access telecommunications data to the offence with more significant penalties.

383. The reference to 'pecuniary penalties' in proposed subparagraph 176A(4)(a)(ii) relates to penalties for breaches of Commonwealth, State and Territory laws that are not prosecuted criminally or that impose a penalty which serves as an administrative alternative

to prosecution (often referred to as civil or administrative penalty provisions). Pecuniary penalties for the purposes of this provision are not intended to encompass small-scale administrative fines.

384. The concept of 'public revenue' in proposed subparagraph 176A(4)(a)(iii) includes State and Territory revenue in addition to Commonwealth revenue. Lawful obligations charged on a regular basis such as taxes, levies, rates and royalties are also included but occasional charges, such as fines, are not. 'Protecting the public revenue' will also include the activities of agencies and bodies undertaken to ensure that those lawful obligations are met; for example routine collection, audits, investigatory and debt recovery actions.

385. The term 'revenue' is not intended to be limited to incoming monies from taxation but could also extend to 'monies which belong to the Crown, or monies to which the Crown has a right, or monies which are due to the Crown'.20 The term 'protection of public revenue' is intended to extend to protecting the revenue from which compensation or similar payments are paid, including circumstances where it is sought to ensure that wrongful payments are not made out of that revenue. The term does not include activities aimed at identifying and eliminating inefficient but lawful spending of public monies. The concept of 'administering' a law in subparagraphs 176A(4)(a)(ii) and (iii) will also include bodies whose functions include investigating possible breaches of relevant laws as this work plays an important role in carrying legislation into effect (including by ensuring that the obligations imposed by the legislation are carried out).

386. The meaning of 'enforcement of the criminal law', for the purposes of subparagraph 176A(4)(a)(i), will include the process of investigating crime and prosecuting criminals. It will also include precursory and secondary intelligence gathering activities which support the investigating and prosecution of suspected offences. The term 'criminal law' includes any Commonwealth, State or Territory law that makes particular behaviour an offence punishable by fine or imprisonment.

387. New subsection 176A(3) will also enable the Minister to declare certain persons specified in the declaration to be 'officers' of the criminal law-enforcement agency. Under the TIA Act, officers, as defined in subsection 5(1) of the Act, have various roles and responsibilities. For example, under section 185C of the TIA Act, evidentiary certificates relating to acts by enforcement agencies may be issued by a certifying officer of that agency. Enabling persons to be declared as officers of a particular enforcement agency will facilitate the effective operation of the TIA Act in relation to that agency.

388. Decisions about declarations are not subject to review under the Administrative Decisions Judicial Review Act 1977 (the ADJR Act) as decisions under the TIA Act are not decisions to which the ADJR Act applies (see paragraph (d) of Schedule 1 to the ADJR Act). The exclusion of these decisions from the ADJR Act does not prevent decisions made under the TIA Act from being judicially reviewed under paragraph 75(v) of the Constitution. Declarations under subsection 176A(3) are also subject to parliamentary review as they are legislative instruments under the Legislative Instruments Act 2003 and can be disallowed under Part 5 of that Act.

389. New subsection 176A(8) will enable the Minister to revoke a declaration made under subsection (3) if the Minister is no longer satisfied that the circumstances justify the

[20] *Stephens v Abrahams* (1902) 27 VLR 753 at 767; see also *Lush v Coles* (1967) 2 All ER 585 at 588.

declaration remaining in force. New subsection 176A(8) will ensure that only agencies with a demonstrated need for telecommunications data will be able to authorise service providers to disclose this information.

390. Under new subsection 176A(9) revocation of a declaration will not affect the validity of an authorisation made by the authorised officer of an authority or body immediately before the revocation took effect. This provision will allow authorities and bodies to rely on authorisations already issued and will protect carriers who act on an authorisation before becoming aware of the revocation.

PART 2—OTHER AMENDMENTS

Telecommunications (Interception and Access) Act 1979

Item 5—Subsection 5(1) (definition of *Crime and Misconduct Commission*)

391. Subsection 5(1) of the TIA Act defines the term *Crime and Misconduct Commission* as meaning the Crime and Misconduct Commission of Queensland. On 1 July 2014, the Crime and Misconduct Commission became the Crime and Corruption Commission under the *Crime and Misconduct and Other Legislation Amendment Act 2014 (Qld)*.

392. Item 5 will amend the definition of *Crime and Misconduct Commission* in subsection 5(1) of the TIA Act to recognise the Commission's change of name.

Item 6—Subsection 5(1) (definition of *criminal law-enforcement agency*)

393. Item 6 will repeal the definition of 'criminal law-enforcement agency' in subsection 5(1) of the TIA Act and replace it with the definition of 'criminal law-enforcement agency' in section 110A.

394. Item 6 is consequential to Item 3 of Part 1 of Schedule 2, which will insert the new definition of 'criminal law-enforcement agency' in section 110A into the TIA Act.

Item 7—Subsection 5(1) (definition of *enforcement agency*)

395. Item 7 will repeal the definition of 'enforcement agency' in subsection 5(1) of the TIA Act and replace it with the definition of 'enforcement agency' in section 176A.

396. Item 7 is consequential to Item 4 of Part 1 of Schedule 2, which will insert the new definition of 'enforcement agency' in section 176A into the TIA Act.

Item 8—Subsection 5(1) (at the end of the definition of *officer*)

397. Item 8 will add new paragraphs (n) and (o) to the end of the definition of 'officer' in subsection 5(1) of the TIA Act. The definition of 'officer' specifies the class of persons who may be taken to be officers of certain agencies, eligible Commonwealth authorities or eligible authorities of a State.

398. Paragraph (n) provides that for a criminal law enforcement agency for which a declaration under subsection 110A(3) is in force, an officer is a person specified, or of a kind specified, in the declaration to be an officer of the criminal law enforcement agency for the purposes of the TIA Act. This item is consequential to Item 3 of Part 1 of Schedule 2, which will insert the new definition of 'criminal law-enforcement agency' in section 110A into the TIA Act.

399. Paragraph (o) provides that for an enforcement agency for which a declaration under subsection 176A(3) is in force, an officer is a person specified, or of a kind specified, in the declaration to be an officer of the enforcement agency for the purposes of the TIA Act. This is consequential upon Item 4 of Part 1 of Schedule 2, which will insert the new definition of 'enforcement agency' in section 176A into the TIA Act.

400. Under Chapter 4 of the TIA Act, only authorised officers of an enforcement agency can request telecommunications data from a carrier. Officers must consider the privacy impacts of the disclosure or use of telecommunications information before making an authorisation and must also be satisfied that the disclosure is reasonably necessary for the enforcement of a relevant law. Section 183 of the TIA Act requires that authorisations must be in a prescribed form and comply with any requirements made by the CAC, a statutory position within the Attorney-General's Department currently filled by the First Assistant Secretary, National Security Law and Policy Division. These requirements are set out in the *Telecommunications (Interception and Access) (Authorisations, Notifications and Revocations) Determination 2012*.

Items 9 and 10—Section 107G

401. Section 107G of the TIA Act is an outline to Part 3-1A of the TIA Act which is about preserving stored communications. Item 9 will remove references to 'an enforcement agency or the Organisation' in section 107G and substitute references to 'a criminal law-enforcement agency, or the Organisation'. Item 10 will remove references to 'an interception agency or the Organisation' in section 107G and substitute references to a 'criminal law-enforcement agency that is an interception agency, or the Organisation'.

402. Items 9 and 10 are consequential to Item 3 of Part 1 of Schedule 2, which will insert the new definition of 'criminal law-enforcement agency' in section 110A into the TIA Act.

Item 11—Subsection 107J(1) (heading)

403. Section 107J of the TIA Act contains the heading 'Notices given by enforcement agencies or interception agencies'.

404. Item 11 will repeal this heading and substitute the heading 'Notices given by criminal law-enforcement agencies.'

405. Item 11 is consequential to Item 2 of Part 1 of Schedule 2 which will delete the reference to 'an enforcement agency' in subsection 110(1) of the TIA Act.

Item 12—Paragraphs 107L(2)(a), 107M(1)(a), (2)(a) and (3)(a)

406. Sections 107L and 107M provide arrangements for revoking domestic preservation notices and who may give or revoke domestic preservation notices. Item 12 will repeal all references in those provisions to the term 'enforcement agency' and substitute references to 'a criminal law-enforcement agency'.

407. Item 12 is consequential upon Item 2 of Part 1 of this Schedule which deletes the reference to 'an enforcement agency' in subsection 110(1).

Item 13—Part 3-3 (heading)

408. Part 3-3 is headed 'Access by enforcement agencies to stored communications'.

409. Item 13 will delete this heading and substitute 'Part 3-3—Access by criminal law-enforcement agencies to stored communications. Item 13 is consequential to Item 2 of Part 1

of Schedule 2 which will delete the reference to ‘an enforcement agency’ and substitute ‘a criminal law-enforcement agency’ in subsection 110(1) of the TIA Act.

Item 14—Section 110 (heading)

410. Section 110 of the TIA Act is headed ‘110 Enforcement agencies may apply for stored communication warrants’. Item 14 will repeal this heading and substitute the heading ‘110 Criminal law-enforcement agencies may apply for stored communications warrants’. Item 14 is consequential to Item 2 of Part 1 of Schedule 2 which will delete the reference to ‘an enforcement agency’ and substitute ‘a criminal law-enforcement agency’ in subsection 110(1) of the TIA Act.

Items 15-33, 35-36, 38-39, 41-47—omit references to ‘enforcement agency’ and ‘an enforcement agency’ and substitute references to ‘criminal law-enforcement agency’ and ‘a criminal law-enforcement agency’

411. These items will delete references to ‘enforcement agency’ and ‘an enforcement agency’s’ as they appear in Chapter 3 of the TIA Act and substitute them with references to ‘criminal law-enforcement agency’ and ‘a criminal law-enforcement agency’s’.

412. These items are consequential to the amendments made by Item 2 of Part 1 of Schedule 2, which will delete the reference to ‘an enforcement agency’ and substitute ‘a criminal law-enforcement agency’ in subsection 110(1) of the TIA Act.

Item 34—Section 130 (heading)

413. Section 130 of the TIA Act is headed ‘Evidentiary certificates relating to actions by criminal law-enforcement agencies’. Item 34 will repeal this heading and substitute the heading ‘130 Evidentiary certificates relating to actions by criminal law-enforcement agencies’.

414. Item 34 is consequential to Item 2 of Part 1 of Schedule 2 which deletes the reference to ‘an enforcement agency’ and substitutes ‘a criminal law-enforcement agency’ in subsection 110(1) of the TIA Act.

Item 37—Subsection 135(1) (heading)

415. Subsection 135(1) of the TIA Act is headed ‘Communicating information to the appropriate enforcement agency’. Item 37 will repeal this heading and substitute the heading ‘Communicating information to the appropriate criminal law-enforcement agency’.

416. This amendment is consequential to Item 2 of Part 1 of Schedule 2 which deletes the reference to ‘an enforcement agency’ and substitutes ‘a criminal law-enforcement agency’ in subsection 110(1) of the TIA Act.

Item 40—Section 138 (heading)

417. Section 138 of the TIA Act is headed ‘Employee of carrier may communicate information to the enforcement agency’. Item 40 will repeal this heading and substitute the heading ‘138 Employee of carrier may communicated information to the criminal law-enforcement agency’.

418. Item 37 is consequential to Item 2 of Part 1 of Schedule 2 which deletes the references to ‘an enforcement agency’ and substitutes ‘a criminal law-enforcement agency’ in subsection 110(1) of the TIA Act.

Part 3—Application Provisions

Item 48—Existing domestic preservation notices

419. Item 48 is a transitional provision that will provide that existing domestic preservation notices will continue to be in force after the commencement of Schedule 2, even if the authority or body that gave the notice is not able to give a notice under the TIA Act as amended, because it is not a criminal law-enforcement agency. This provision will allow agencies to rely on notices already issued and will ensure that carriers do not unlawfully access stored communications.

Item 49—Existing stored communications warrants

420. Item 49 is a transitional provision that will provide that existing stored communications warrants will continue to be in force after the commencement of Schedule 2, even if the authority or body that obtained the warrant is not able to obtain the warrant under the TIA Act as amended, because it is not a criminal law enforcement agency. This provision will allow agencies to rely on warrants already issued and will ensure that carriers do not unlawfully access stored communications.

Item 50—Existing authorisations

421. Item 50 is an application provision that will provide that existing authorisations will continue to be in force after the commencement of Schedule 2, even if the authority or body that made the authorisations is not able to make authorisations under the TIA Act as amended, because it is no longer an enforcement agency.

422. This provision will allow agencies to rely on authorisations already issued and will ensure that carriers do not unlawfully disclose information or documents the disclosure of which would otherwise be prohibited under section 276, 277 or 278 of the *Telecommunications Act 1997*.

Item 51—Evidentiary certificates

423. Subitem (1) will provide that an evidentiary certificate issued by an authority or body under section 107U or 130 of the TIA Act continues to be in force even if on the commencement of Schedule 2 the authority or body ceases to be a criminal law-enforcement agency.

424. Subitem (2) will provide that an evidentiary certificate issued by an authority or body under section 185C of the TIA Act will continue to be in force even if on the commencement of Schedule 2 the authority or body ceases to be an enforcement agency.

425. Subitem (3) will provide that an authority or body that ceases to be a criminal law-enforcement agency upon the commencement of Schedule 2 will be able to issue evidentiary certificates under section 107U or 130 of the TIA Act with respect to anything done before the commencement of Schedule 2.

426. Subitem (4) will provide that an authority or body that ceases to be an enforcement agency upon the commencement of Schedule 2 will be able to issue evidentiary certificates under section 107U or 130 of the TIA Act with respect to anything done before the commencement of Schedule 2.

427. Item 51 is an application provision which will ensure that evidentiary certificates do not become invalid upon the commencement of this Act. Evidentiary certificates are received as evidence of facts in prosecutions and civil penalty court proceedings and the amendments contained in this item will ensure that court proceedings are not adversely impacted by a change in an authority or body's status when this Act commences.

SCHEDULE 3—OVERSIGHT BY THE COMMONWEALTH OMBUDSMAN

Overview of measures

428. Schedule 3 will amend the TIA Act by inserting new obligations to keep records in relation to the access of stored communications (Chapter 3 of the TIA Act) and telecommunications data (Chapter 4 of the TIA Act). The Bill will insert a new Chapter 4A to implement a comprehensive record-keeping, inspection and oversight regime in relation to:

- the issue of preservation notices by criminal law-enforcement agencies
- the access to, and dealing with, stored communications by criminal law-enforcement agencies, and
- the access to, and dealing with, telecommunications data by criminal law-enforcement agencies and enforcement agencies.

429. The new record-keeping regime will require all Commonwealth, State and Territory enforcement agencies to keep prescribed information and documents necessary to demonstrate that they have exercised their powers under Chapters 3 and 4 in accordance with their statutory obligations under the TIA Act. The specificity of the oversight provisions is intended to provide sufficient clarity to enable agencies to be properly versed as to what the Ombudsman would require to be kept and made available at inspections.

430. The new inspection and oversight regime will then require the Ombudsman to inspect and oversight the records of Commonwealth, State and Territory agencies in order to assess compliance against the exercise of their powers under Chapters 3 and 4 of the TIA Act.

431. Currently, the TIA Act does not provide for independent oversight for the use of, and access to, telecommunications data by enforcement agencies. Under the TIA Act, the Ombudsman has limited audit functions to assess the compliance by agencies with record keeping and record destruction obligations in relation to the issue of preservation notices and access to stored communications. While carrying out such an audit, other compliance issues may come to the Ombudsman's attention, but these would not expressly fall within the Ombudsman's existing inspection remit under the TIA Act. While the Ombudsman is empowered to report on these additional compliance issues (by virtue of the existing 'incidental or conducive to the performance' of functions provision in section 152), the extent of the Ombudsman's power is not clearly delineated.

432. The IGIS currently inspects and reports on access to telecommunications data by ASIO, under the *Inspector-General of Intelligence and Security Act 1986*.

433. The proposed oversight regime will be similar to the existing Ombudsman oversight model contained in Part 6 of the *Surveillance Devices Act 2004* (SD Act), and will enable comprehensive assessment of agency compliance with all of an enforcement agency's (or a criminal law-enforcement agency's) obligations under Chapters 3 and 4 of the TIA Act, including access to and use of telecommunications data, which can be accessed on a

historical basis (sections 178, 178A, 179) and on a prospective (or near-real time) basis (section 180). Oversight of this category of data would, by extension, capture the set of telecommunications data that service providers will be required to retain under proposed subsection 187A of the Act.

434. The proposed provisions relating to the powers, scope and reporting obligations of the oversight role are intended to enable the Ombudsman to provide public assurance and to enhance levels of transparency and public accountability. These provisions would also align with other oversight roles performed by the Ombudsman, such as those performed under the SD Act and the Controlled Operations provisions in Part IAB of the *Crimes Act 1914*.

435. Part 1 of this Schedule contains the main amendments to Chapters 3 and 4, as well as minor and consequential amendments to Chapters 1 and 2. These main amendments will introduce new record-keeping obligations for criminal law-enforcement agencies and enforcement agencies, and will establish a comprehensive oversight regime administered by the Ombudsman for such agencies accessing stored communications and telecommunications data.

436. Part 2 of this Schedule provides for how the amendments contained in Schedule 3 apply upon their commencement.

PART 1—AMENDMENTS

Telecommunications (Interception and Access) Act 1979

Item 1—Subsection 5C(1)

437. Item 1 will amend section 5C of the TIA Act, which defines when information or a question is relevant to an inspection by the Ombudsman. The clause will delete the reference to 'Part 3-5' in subsection 5C(1) of the TIA Act and substitute a reference to new Chapter 4A of the TIA Act.

438. This is a technical amendment to ensure that the definition of when information or a question is relevant to an Ombudsman inspection refers to the provisions of the Act which pertain to Ombudsman oversight, which will be contained in Chapter 4A.

Item 2—At the end of section 87

439. Section 87 of the TIA Act sets out the powers the Ombudsman has to obtain relevant information, in documentary or oral form, in relation to an Ombudsman inspection of the use of interception powers by Commonwealth agencies in circumstances where the Ombudsman has reason to believe that an officer of an agency is able to give information relevant to an inspection under Part 2-7 and relating to that agency's records.

440. This item will insert a new subsection 87(6) into the TIA Act that would make it a criminal offence for a person to refuse to attend, give information or answer questions in relation to such an inspection.

441. The penalty for an offence against proposed subsection 87(6) will be six months imprisonment.

442. Proposed subsection 87(6) will mirror proposed subsection 186C(3) (applicable to stored communications and telecommunications data) in terms of the form of the offence and the applicable penalty. It is also broadly consistent with similar provisions under the *Surveillance Devices Act 2004* (section 56) and the *Inspector-General of Intelligence and Security Act 1986* (section 18). The proposed offence provision will only be enlivened in relation to officials of law enforcement agencies. Such officials hold positions of public trust and exercise intrusive and covert powers under the TIA Act. Accordingly, public confidence in the justice system requires that officials are held to a higher standard of conduct, particularly because there are fewer avenues to identify misconduct or systemic non-compliance in the telecommunications interception environment due to its covert nature.

Item 3—Section 134

443. This item will amend section 134 of the TIA Act, which sets out when a person may deal in preservation notice information or stored communications warrant information.

444. The amendment will provide that a person may deal in such information for the purposes of new Chapter 4A of the TIA Act (Oversight by the Commonwealth Ombudsman). The purpose of this provision would be to clarify that dealing with preservation notice information and stored communications information will be permitted if it is for the purposes of an Ombudsman inspection under new Chapter 4A of the TIA Act.

Item 4—Part 3-5 (heading)

445. This item will repeal the heading to Part 3-5 ('Keeping and inspection of preservation notices and access records') and substitute a new heading ('Keeping and inspection of records'). The new heading is a technical amendment to reflect the amendments to Part 3-5 in the Bill. While the current Part 3-5 of the Act contains both record keeping obligations on agencies and an inspection regime by the Ombudsman, the amended Part 3-5 of the Act will be limited to placing inspection obligations on criminal-law enforcement agencies (although section 158A of the TIA Act will remain). The change in the heading to Part 3-5 will reflect this extended remit.

Item 5—New section 151 of Division 1 of Part 3-5: Obligation to keep records

446. This item would repeal Divisions 1 and 2 of Part 3-5 and substitute a new Division 1 of Part 3-5.

447. Division 1 of Part 3-5 currently describes the records that enforcement agencies must keep in relation to their use of preservation notices and the use of powers to access stored communications.

448. Division 2 of Part 3-5 currently sets out a regime for inspection of record keeping by enforcement agencies relating to preservation notices and access to stored communications.

449. Repealing Divisions 1 and 2 and substituting new Division 1 is necessary so that auditing of stored communications can be undertaken in a manner consistent with the proposed approach to the oversight of other powers exercisable under Chapter 4 of the TIA Act.

450. Section 151 will comprehensively set out the information or documents that a criminal law-enforcement agency must retain to enable the Ombudsman to inspect the agency's records to determine the extent of its compliance with Chapter 3 of the TIA Act. Chapter 3 of the Act relates to the issue of preservation notices and the access to and dealing with stored communications.

451. The purpose of section 151 is to ensure that agencies retain the records that the Ombudsman will require in order to carry out his or her inspection functions under proposed new Chapter 4A of the TIA Act.

452. An agency will be able to meet the requirements of section 151 by retaining either the original or a copy of the relevant document.

453. Subsection 151(2) will provide that the Minister may, by legislative instrument, prescribe the kinds of documents and other materials that the chief officer of a criminal law-enforcement agency must cause to be kept in the agency's records. The requirement for additional records to evidence compliance will be prospective. Further prescription of documents by legislative instrument will enable the record keeping list for the purpose of compliance assessment to expand over time if it is deemed additional record keeping requirements are required to enable the Ombudsman to determine agencies' compliance.

454. Subsection 151(3) will specify how long agencies must retain records for compliance inspection purposes. This provision would require agencies to retain the records referred to in subsection 151(1) and any documents or other materials prescribed under subsection 151(2) for a maximum of 3 years from when the document or record came into existence (subparagraph 151(3)(b)(i)) or until the Ombudsman gives a report to the Minister under section 186J that is about records that include that particular record (subparagraph 151(3)(b)(ii)), whichever happens earlier. Requiring agencies to keep records until the Ombudsman has made findings on, and made reports in relation to, those records, would functionally meet the Ombudsman's requirements for when they would no longer require the records for inspection purposes. The proposed maximum retention period of three years is consistent with the period currently contained in section 185 of the TIA Act for the retention of data authorisations made under Divisions 4 and 4A of Part 4-1. The proposed approach would also avoid imposition of arbitrary and discordant retention timeframes on agencies across record types.

Item 6—New section 186A: Obligation to keep records

455. Proposed new section 186A would set out the information or documents that an enforcement agency must retain to ensure that the Ombudsman is able to inspect the agency's records to determine the extent of the agency's compliance with Chapter 4 of the TIA Act. Chapter 4 of the Act relates to the access to and dealing with telecommunications data by enforcement agencies.

456. An agency can meet the requirements of section 186A by retaining either the original or a copy of the relevant document.

457. Proposed subsection 186A(2) will allow the Minister to prescribe kinds of documents and other materials that a criminal law-enforcement agency must keep in addition to those specified under subsection 186A(1). This will be a legislative instrument for the purposes of the *Legislative Instruments Act 2003*. Subsection 186A(2) will operate in conjunction with

new paragraph 186A(1)(j) of the TIA Act, which will require criminal law-enforcement agencies to retain such records.

458. The purpose of subsection 186A(2) and related paragraph 186A(1)(j) will be to require new classes of documentation to be kept in future as the new inspection regime develops. It will also accommodate the addition of new types of documents to be retained if the powers and functions of relevant agencies and the Ombudsman change.

459. Subsection 186A(3) will specify how long agencies must retain records for compliance inspection purposes. This provision would require agencies to retain the records referred to in paragraphs 186A(1)(a)-(i) or other materials prescribed under subsection 186A(2) for a maximum of 3 years from when the document or record came into existence (paragraph 186A(3)(b)(i)) or when the Ombudsman gives a report to the Minister under section 186J that is about records that include that particular record (paragraph 186A(3)(b)(ii)), whichever happens earlier. Requiring agencies to keep records until the Ombudsman has made findings on, and made reports in relation to those records, would functionally meet the Ombudsman's requirements for when they would no longer require the records for inspection purposes. The proposed maximum of three years is consistent with the period currently contained in section 185 of the TIA Act for the retention of data authorisations made under Divisions 4 and 4A of Part 4-1. However, the retention period referred to in subsection 186A(3) will not affect the operation of the retention period section 185, which will still apply.

Item 7—Chapter 4A: Oversight by the Commonwealth Ombudsman

460. Item 7 inserts new Chapter 4A before Chapter 5 of the TIA Act. Chapter 4A sets out a new oversight regime for the Commonwealth Ombudsman.

New section 186B—Inspection of records

461. Section 186B will establish an inspection regime to enable the Ombudsman to inspect the records kept by enforcement agencies associated with use of, and access to, telecommunications data and stored communications. New sections 151 and 186A will facilitate this inspection regime by requiring agencies to keep such records. The role of the Ombudsman will be to determine whether an agency is compliant with its obligations relating to the issue of preservation notices and access to stored communications under Chapter 3, and access to telecommunications data under Chapter 4 of the TIA Act.

462. New subsection 186B(1) is not intended to require the Ombudsman, nor to give the Ombudsman the power to, inspect, review or report on whether an issuing authority ought to have issued a stored communications warrant under section 116 of the Act.

463. New paragraph 186B(1)(a) will require the Ombudsman to inspect the records of enforcement agencies to determine the extent of their compliance with the exercise of statutory powers associated with telecommunications data access set out in Chapter 4 of the TIA Act.

464. Access to telecommunications data by enforcement agencies has the potential to impact on the privacy of persons whose data is being accessed. A comprehensive oversight regime for telecommunications data will assist in ensuring that access to, and the use and disclosure of telecommunications data by enforcement agencies, including retained data,

under Chapter 4 of the TIA Act, is subject to independent compliance assessment. It will also serve to provide an important level of public accountability and scrutiny of agency practices by virtue of the Ombudsman public reporting regime proposed to be implemented in Chapter 4A.

465. New paragraph 186B(1)(b) would require the Ombudsman to inspect the records of criminal law-enforcement agencies to determine the extent of their compliance with the requirements set out in Chapter 3 of the TIA Act in relation to the issue of preservation notices and the access to and dealing with stored communications. It also requires the Ombudsman to inspect records of an enforcement agency to determine the extent of compliance with Chapter 4 by the agency and its officers.

466. Tailored oversight provisions in relation to the use by agencies of preservation notices and their access to and dealing with stored communications are important inclusions in the Bill because:

- the use of preservation notices by criminal law-enforcement agencies potentially impacts on individual privacy, in that agencies can use such notices to ensure that carriers and carriage service providers preserve the private stored communications of persons where the agency intends to later apply for an interception or stored communications warrant to access those communications in connection with the investigation of a serious contravention, and
- the access to and dealing with stored communications by criminal law-enforcement agencies also potentially impacts on individual privacy. As such, it is important that access to, and dealing with, such communications occurs only as permitted under the TIA Act.

467. The purpose of an Ombudsman oversight regime in relation to preservation notices and stored communications is to ensure, from a public accountability perspective, that criminal law-enforcement agencies only use such powers strictly in accordance with the statutory requirements under Chapter 3 of the TIA Act. The oversight regime is also intended to reassure the public that agencies are exercising these covert and intrusive powers in accordance with the law.

468. Proposed subsection 186B(2) will provide that the Ombudsman, for the purpose of an investigation under subsection 186B(2), can enter premises occupied by an agency at any reasonable time after notifying the chief officer of the agency. The Ombudsman is then entitled to full and unimpeded access at all reasonable times to all records of the agency that are relevant to the Ombudsman's inspection. The Ombudsman will be entitled to make copies of, and take extracts from, the agency's records where relevant to the investigation. The provision will also give the Ombudsman the power to require a member of staff of the agency to provide any information relevant to the inspection that is in their possession or to which the staff member has access.

469. The purpose of new subsection 186B(2) is to ensure the Ombudsman has sufficient powers to carry out the Ombudsman's inspection functions under Chapter 4A in relation to agencies.

470. Under subsection 186B(2), the Ombudsman will not be restricted in the frequency with which the Ombudsman may inspect the records of an agency. For example, the

Ombudsman could choose inspection cycles of twelve months, six months, three months or some other period to inspect the records of any particular agency. This flexibility is intended to cater for the significant differences in the size, structure, functions, and internal systems and procedures of the various criminal law-enforcement agencies, the variable nature and flow of investigations and to ensure the new inspection regime is sufficiently responsive to differing contingencies encountered during an inspection. Depending on the circumstances, this may necessitate other adaptive approaches, including, for example, staged or rolling inspection programs, a quarter-sized inspection four times a year, or inspecting different field offices at different times if that was more convenient for the agency from an operational perspective or logistically more feasible. The current stored communications inspection regime under the TIA Act and the regime under the SD Act do not cap the number of inspections, and proposed section 186B is consistent with those existing statutory frameworks.

471. Subsection 186B(3) will require the Ombudsman to give the chief officer of an enforcement agency reasonable notice of an inspection under subsection 186B(2).

472. Subsection 186B(4) will require the chief officer of an agency to ensure that his or her staff provide the Ombudsman with any assistance that the Ombudsman reasonably requires to enable the Ombudsman to perform his or her functions under new section 186B. The purpose of proposed subsection 186B(4) is to ensure that agency staff provide reasonable cooperation to the Ombudsman in relation to the Ombudsman carrying out his or her statutory inspection functions.

473. Subsection 186B(5) will provide that subsection 186B(1) does not require the Ombudsman to inspect all of the information or documents which could conceivably come under the auspices of paragraphs 186B(1)(a) and (b). As proposed subsection 186B(1) provides that the Ombudsman 'must' inspect the records of an agency to determine the extent of compliance by the agency with Chapter 3 or Chapter 4 of the TIA Act, proposed subsection 186B(5) serves as an avoidance of doubt clause to qualify the directive obligation set out in proposed section 186B(1).The purpose of this subsection would be to make it clear that the Ombudsman can use any appropriate inspection methodology (for example, sampling as indicative of compliance across a particular record field, or focusing the majority of the Ombudsman's attention on areas considered to be higher risk). The subsection is also intended to clarify that the Ombudsman will have the discretion to inspect records the Ombudsman considers to be appropriate in fulfilling its inspection functions under new Chapter 4A, and is not required to inspect every record held by an agency.

474. In addition, subsection 186B(5) is not intended to impact upon, or result in a diminution of, the Ombudsman's inspection function under subsection 186B(1).

475. Subsection 186B(6) will provide that the Ombudsman may choose to refrain from inspecting records of an agency that concern the obtaining or the execution of a stored communications warrant or telecommunications data authorisation while an ongoing operation is being conducted in relation to that warrant or authorisation.

476. The purpose of subsection 186B(6) will be to ensure that inspections will not interfere with the progress of a current operation. This provision is intended to avoid inspections occurring at an intermediate juncture when operations being conducted under a stored communications warrant or an authorisation under Division 3, 4 or 4A of Part 4-1 of the

TIA Act are actively being progressed. Inspecting records at these times could potentially hamper the conduct of proceedings or impede the progress of investigations. Further, the inspection results may be improperly calibrated because they would measure compliance before critical events have occurred in respect of the issuing, or execution of a warrant or may occur during the course of obtaining an emergency or tracking device authorisation.

New section 186C—Power to obtain relevant information

477. Proposed section 186C will empower the Ombudsman to require an officer of an enforcement agency to provide information to the Ombudsman in writing, signed by the officer, at a specified place and within a specified period of time where the Ombudsman has reason to believe that the officer is able to give the information required.

478. The purpose of section 186C will be to ensure that the Ombudsman has sufficient power to carry out the Ombudsman's inspection functions under new Chapter 4A and can acquire supplementary information where necessary to effectively conduct an investigation, including by requiring officers of an agency to attend and answer relevant questions.

479. Under paragraph 186C(1)(a), if the Ombudsman knows the officer's identity, the Ombudsman must write to the officer in order to require the officer to provide the written information and/or attend to answer questions.

480. Paragraph 186C(1)(b) will apply when the Ombudsman does not know the identity of the relevant officer in an agency. In these circumstances, the provision will authorise the Ombudsman to write to the chief officer of an enforcement agency to require them, or a person nominated by the chief officer, to answer questions relevant to the inspection before a specified inspecting officer, at a specified place and within a specified period, or at a particular time on a particular day, which is reasonable having regard to the circumstances.

481. Subsection 186C(2) will provide that the Ombudsman must specify a place and time for an officer to attend as required under subsection 186C(1). The place and time nominated must be reasonable in the circumstances.

482. Subsection 186C(3) will establish an offence where a person refuses to attend before a person, give information or answer questions when required to do so under section 186C. The maximum penalty for the offence will be imprisonment for six months.

483. The purpose of an offence provision under subsection 186C(3) will be to ensure that agency officers do not hinder the Ombudsman inspection functions under Chapter 4A of the TIA Act by unreasonably refusing to attend, give information or answer questions as required. It is also broadly consistent with similar provisions under the *Surveillance Devices Act 2004* (section 56) and the *Inspector-General of Intelligence and Security Act 1986* (section 18). The proposed offence provision will only be enlivened in relation to officials of law enforcement agencies. Such officials hold positions of public trust and exercise intrusive and covert powers under the TIA Act. Accordingly, public confidence in the justice system requires that officials are held to a higher standard of conduct, particularly because there are fewer avenues to identify misconduct or systemic non-compliance in the telecommunications interception environment due to its covert nature.

New section 186D—Ombudsman to be given information and access despite other laws

484. Section 186D will provide that a person is to be given information and access to documents despite other laws, including the laws of any State or Territory. The purpose of this provision is to ensure that the Ombudsman is able to obtain all the information and documents required to carry out the Ombudsman's inspection functions under the TIA Act, and that agency officers are not prevented by other laws from providing necessary information or assistance.

485. Subsection 186D(1) will provide that a person is not excused from giving information, answering a question or giving access to a document (disclosing information), as required under Chapter 4A (oversight by the Commonwealth Ombudsman) of the TIA Act, despite other matters which may otherwise bar the giving of that information.

486. These matters are listed at paragraphs 186D(1)(a) to (c) and are that disclosure of the information would be: a contravention of a law (including the law of any State or Territory); contrary to the public interest, or might tend to incriminate the person or make the person liable to a penalty.

487. Paragraph 186D(1)(c) will abrogate the privileges against self-incrimination or self-exposure to a civil or administrative penalty (hereinafter referred to together as 'self-incrimination') in relation to the disclosure of information required under Chapter 4A.

488. Subsection 186D(2) will however provide that the disclosed information cannot be used as evidence against the person who disclosed that information, whether directly or indirectly (a 'use immunity' and 'derivative use' immunity). The use and derivative use immunity does not apply to prosecutions for offences against sections 133, 181A, 181B and 182 of the TIA Act or Part 7.4 or 7.7 of the Criminal Code.

489. Section 133 of the TIA Act creates an offence of unlawful dealing in accessed stored communications under Chapter 3, Part 3-4, Division 1 of the TIA Act. Sections 181A, 181 and 182 create offences for unlawful dealing in telecommunications data authorisation information or unlawful secondary disclosure of accessed telecommunications data under Chapter 4, Part 4-1, Division 6 of the TIA Act. Parts 7.4 (false or misleading statements) and Part 7.7 (forgery and related offences) of the Criminal Code create offences relating to hindering, obstructing, intimidating or resisting a public official in the performance of their functions.

490. The use and derivative use immunity will not prevent the admission of disclosed information as evidence against a person other than the person who disclosed the information.

491. The immunity is an important human right. However, the public interest in abrogating the privilege outweighs the interest in maintaining the privilege. First, the powers to access stored communications and telecommunications data are intrusive and covert powers, the unlawful use or disclosure of which could potentially result in significant harm to individuals, including a significant intrusion on their privacy. There is, therefore, a strong public interest in the Ombudsman, being the relevant oversight body for these powers, to be able to compel an officer of an enforcement agency to reveal information that might indicate that stored communications or telecommunications data have been unlawfully used or

disclosed, even if doing so would show that the person had committed an offence, or might be liable to a penalty.

492. Second, the integrity of the stored communications and telecommunications data regimes, and public confidence therein, are important in their own right. The powers afforded to agencies under these regimes are key investigative tools for a range of serious criminal offences, the investigation of which are manifestly in the public interest. Officers exercising these powers are afforded a high degree of public trust, given their intrusive and covert nature. A serious breach of the integrity of the regime, and/or a loss of confidence therein (including a loss of confidence based on a perception of a lack of integrity,) would create a serious risk that these powers would be fettered or removed, to the detriment of agencies' investigative capabilities. It is, therefore, important that the Ombudsman have the power to compel an officer of an enforcement agency to reveal information that might indicate that stored communications or telecommunications data have been unlawfully used or disclosed, and to be seen to have such a power, even if doing so would show that the person had committed an offence, or might be liable to a penalty.

493. Third, the abrogation of the privilege occurs within the context of a regulatory regime, and applies only to people who are voluntarily subject to that regime, being in all cases people who have chosen to be officers of enforcement agencies and, in most cases, officers who have chosen to be involved in, or in relation to the exercise of these powers under Chapters 3 and 4 of the TIA Act.

494. The harm to individual rights is minimised by the provision of a use and derivative use immunity. The immunity is however limited, and does not apply to proceedings for specific offences, prosecutions and civil penalties under the TIA Act and certain Criminal Code offences.

495. The regime contained in Chapter 4A will strengthen oversight and accountability of agency access to stored communications and telecommunications data. The benefit to the public of an effective oversight regime is high, given the privacy sensitive nature of this information. The disclosure of information to the Commonwealth Ombudsman, and the ability to prosecute a person involved in wrongdoing under the TIA Act, forms a core part of the inspection and oversight functions of the Ombudsman. This function would be significantly impaired if persons were excused from providing self-incriminating information, or if that information could not be used as evidence in TIA Act proceedings.

496. Other laws do not prevent the disclosure of information for the purposes of an inspection. Subsections 186D (3) and (4) will provide that the unlawful disclosure provisions in sections 133, 181A, 181B or 182 of the TIA Act or in any other law will not prevent the disclosure of information to an inspecting officer of the Commonwealth Ombudsman for the purposes of an inspection under the oversight provisions contained in new Chapter 4A.

497. The purpose of provisions such as those in sections 133, 181A, 181B or 182 of the TIA Act is to protect the privacy of impact on persons whose information was accessed under the TIA Act. Given the purpose of the oversight regime in ensuring that agencies access this privacy sensitive information in a lawful manner, it is appropriate that the requirement to disclose information to the Ombudsman under section 186D overrides any other laws that prevent the disclosure of that information. Subsection 186D(3) will provide that nothing in sections 133, 181A, 181B or 182 of the TIA Act or any other law prevents an

officer of an enforcement agency from providing information to an inspecting officer in any form or from providing access to records of the enforcement agency for the purposes of an inspection under new Chapter 4A.

498. Subsection 186D(4) will also provide that nothing in sections 133, 181A, 181B, 182 of the TIA Act or any other law, prevents an officer of an enforcement agency from making a record of information, or causing such a record to be made for the purposes of giving the information to a person as permitted by subsection 186D(3).

New section 186E—Application of Ombudsman Act

499. Section 186E will set out the interaction of the *Ombudsman Act 1976* (Cth) (the Ombudsman Act) with the new Ombudsman oversight regime in Chapter 4A of the TIA Act. The purpose of this provision is to ensure that the specific powers and duties of the Ombudsman in new Chapter 4A interact correctly and appropriately with the general powers and duties of the Ombudsman in the Ombudsman Act.

500. Subsection 186E(1) will provide that section 11A of the Ombudsman Act, regarding the power of the Federal Court of Australia to determine matters concerning the Ombudsman's powers, does not apply to the proposed exercise of a power or function by the Ombudsman under new Chapter 4A.

501. Subsection 186E(2) will provide that section 19 of the Ombudsman Act, regarding annual reporting to Parliament, does not apply to any act or omission of an Ombudsman inspecting officer under new Chapter 4A.

502. Subsection 186E(3) will provide that, subject to section 186D (which provides that the Ombudsman is to be given information and access despite other laws), sections 35(2), (3), (4) and (8) of the Ombudsman Act (regarding the preservation of confidentiality of inspecting officers) apply for the purposes of new Chapter 4A.

New section 186F—Exchange of information between Ombudsman and State inspecting authorities

503. Section 186F will allow the Ombudsman to develop more effective and consistent inspection arrangements with State and Territory inspection authorities, including State or Territory Ombudsmen. The purpose of new section 186F is to ensure that the Ombudsman and State and Territory inspecting authorities (including State and Territory Ombudsmen) can exchange information with each other that is relevant to their inspection functions.

504. Subsection 186F(1) will enable the Ombudsman to give information that relates to an authority of a State or Territory, which was obtained by the Ombudsman under the TIA Act, to the inspecting authority in relation to the agency in the relevant State or Territory.

505. Subsection 186F(2) will qualify subsection 186F(1) by providing that the information can only be passed where the Ombudsman believes the information is necessary for the inspecting authority to perform its functions in relation to the State or Territory agency.

506. Subsection 186F(3) will also provide that the Ombudsman can receive from an inspecting authority information relevant to the performance of the Ombudsman's functions under the TIA Act.

New section 186G—Delegation by Ombudsman

507. Section 186G will provide for the Ombudsman's powers of delegation. The purpose of this provision is to ensure that members of the staff of the Ombudsman's office can perform the functions of the Ombudsman as required. It is envisaged that the functions of the Ombudsman would be carried out by members of the Ombudsman's staff under a *Carltona* type delegation. *Carltona* delegates would act in the name of the person making the delegation—the Ombudsman. The delegation provisions would not preclude the Ombudsman from making an ordinary statutory delegation of powers.

508. Subsection 186G(1) will provide that the Ombudsman may delegate the Ombudsman's powers under Chapter 4A to an Australian Public Service (APS) employee responsible to the Ombudsman (which may include, for example, an employee of another APS agency seconded to the Ombudsman's office) or an employee of a State or Territory oversight body that has similar oversight functions to the Commonwealth Ombudsman.

509. Subsection 186G(1) will also provide that the Ombudsman does not have the power to delegate the power to report to the Minister as set out in proposed section 186J. In addition, the Ombudsman's power to delegate would not include the power of delegation set out in proposed subsection 186G(1).

510. A delegation by the Ombudsman under subsection 186G(1) will not prevent the exercise of that power by the Ombudsman.

511. Subsection 186G(2) will provide that a delegate must produce, upon the request of any person affected by an exercise of power under a delegation under s186G(1), the instrument to the person (or a copy of the instrument). It will be possible for the delegate to satisfy this requirement by producing an electronic copy of the delegation.

New section 186H—Ombudsman not to be sued

512. Proposed section 186H will give immunity from suit to the Ombudsman, an inspecting officer or a person acting under an inspecting officer's authority, for an act or omission made in good faith in the performance of the Ombudsman's inspection functions under new Chapter 4A.

513. The purpose of section 186H will be to ensure that the Ombudsman and the Ombudsman's staff are able to perform their inspection functions under new Chapter 4A without being impeded by the possibility of legal action. However, this immunity will only apply if the inspection functions are being carried out in good faith.

New section 186J—Reports

514. Section 186J will implement a new public reporting regime in relation to the Ombudsman's oversight functions set out under section 186B. The Ombudsman will be required to report on the results of its oversight functions relating to compliance by agencies generally with the requirements of Chapters 3 and 4 of the TIA Act relating to issue of preservation notices, access to stored communications and access to telecommunications data.

515. One of the purposes of section 186J is to ensure that the Ombudsman is able to make public the results of its inspections under new Chapter 4A. Public reporting by the Ombudsman is a key element in providing public accountability and transparency in relation to the use by agencies of their powers under Chapters 3 and 4 of the TIA Act. It is also designed to reassure the public that agencies are using their powers under Chapters 3 and 4 of the TIA Act lawfully and appropriately.

516. Subsection 186J(1) will provide that the Ombudsman must provide a written report to the Minister containing the results of the inspections undertaken under new section 186B of the TIA Act.

517. Subsection 186J(2) will provide that the Ombudsman must give the Minister the report as soon as practicable by the end of each financial year. This gives the Ombudsman's inspectors some further latitude given the wide ranging compliance assessments that need to be conducted across a range of agencies against all powers potentially exercisable under Chapters 3 and 4. An extended timeframe may be required, particularly with the introduction of the mandatory data retention regime, which may collaterally impact upon the time needed to conduct, and the complexity of, compliance assessment.

518. Subsection 186J(3) will provide that a copy of the Ombudsman's report is to be tabled by the Minister before each House of Parliament within 15 sitting days of that House after the Minister has received the report.

519. Subsection 186J(4) will provide that the Ombudsman can report to the Minister at any time and also that the Minister may require the Ombudsman to do so. The purpose of this provision is to clarify that the Ombudsman is not restricted to providing reports to the Minister only at twelve monthly intervals. For example, the Ombudsman could choose to report more frequently in relation to a particular agency. This is consistent with the provisions in proposed section 186B which provide that the Ombudsman may inspect the records of an agency at any time.

520. Subsection 186J(4) will also clarify that the Minister can require the Ombudsman to report to the Minister on an inspection by the Ombudsman under new Chapter 4A.

521. Subsection 186J(5) will provide that the Ombudsman can include in an inspection report any suspected contravention of the TIA Act by an officer of an enforcement agency the Ombudsman has inspected. The purpose of this is to ensure that the Ombudsman has a general power to report on purported contraventions of the TIA Act that the Ombudsman discovers in relation to its inspections under Chapter 4A of the Act.

522. A suspected contravention reported by the Ombudsman does not, as a matter of course, give rise to, or imply legal liability. In complying with this section, the Ombudsman is bound by the obligations imposed by sections 133, 181B and 182 of the TIA Act. Section 133 of the TIA Act creates an offence of unlawful dealing in accessed stored communications under Chapter 3, Part 3-4, Division 1 of the TIA Act. Sections 181B and 182 create offences for unlawful dealing in telecommunications data authorisation information or unlawful secondary disclosure of accessed telecommunications data under Chapter 4, Part 4-1, Division 6 of the TIA Act.

523. Subsection 186J(7) will provide that an Ombudsman's report must not contain information that could endanger a person's safety, prejudice an investigation or prosecution,

or compromise an enforcement agency's lawful activities or methods. The purpose of this provision is to ensure that the report does not contain security sensitive information or information which reveals law enforcement capability that should not be made public.

524. Subsection 186J(6) will require the Ombudsman to give a copy of a report to the chief officer of the relevant enforcement agency which is the subject of the report.

PART 2—APPLICATION PROVISIONS

525. Part 2 of Schedule 3 contains application provisions in relation to Ombudsman inspections, Ombudsman reports and the obligation by agencies to retain records for the purposes of Ombudsman inspections.

Item 8—Existing inspections by the Ombudsman

526. Item 8 is an application provision. It will provide that Ombudsman inspections in existence before the commencement of Schedule 3, but not yet completed, will be treated as Ombudsman inspections conducted as if they were being conducted under the new regime in Chapter 4A of the TIA Act. The provision will also provide that anything done under the inspection before the commencement of new Chapter 4A will be deemed to have been done under new Chapter 4A.

527. The purpose of this provision will be to ensure that existing Ombudsman inspections still in progress prior to the commencement of the new inspection regime in Chapter 4A remain valid.

Item 9—Reports

528. Item 9 is an application provision. It will apply to Ombudsman inspections under the current section 152 of the TIA Act that had been completed prior to the commencement of the new inspection regime, but which the Ombudsman had not yet reported on under current section 153 of the TIA Act. The provision will apply the reporting provisions in new section 186J to these circumstances.

529. The purpose of this item will be to ensure that the Ombudsman can still report on material for which it had completed an inspection under the current section 152, but had not yet been able to provide a report under current section 153 of the TIA Act.

Item 10—Obligation to keep records

530. Item 10 is an application provision. It would provide that the new record keeping provisions in relation to Ombudsman inspections in sections 151 and 186A do not apply to anything done before commencement of the new inspection regime in Chapter 4A of the TIA Act. The purpose of this is to clarify that agencies are not required to comply with the more detailed record keeping obligations in proposed sections 151 and 186A of the TIA Act in relation to their use of powers under Chapters 3 and 4 of the TIA Act prior to the commencement of the new Ombudsman inspection regime.

531. The item will also provide that the record keeping provisions in the current 150A of the TIA Act (relating to preservation notices) and section 151 of the TIA Act (relating to stored communications access) continue to apply to anything done prior to the

commencement of the new inspection regime. The purpose of this would be to ensure that enforcement agencies (as that term applied under the TIA Act prior to the commencement of this legislation) still have to comply with the record keeping provisions in current sections 150A and 151 of the TIA Act in relation to the use of powers in Chapter 3 of the TIA Act prior to the commencement of the new Ombudsman inspection regime.