2013-2014-2015

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

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

SUPPLEMENTARY EXPLANATORY MEMORANDUM

Amendments

to be Moved on Behalf of the Government

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

AMENDMENTS TO THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT (DATA RETENTION) BILL 2014

GENERAL OUTLINE

1. The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) was introduced in the House on 30 October 2014 and was referred to the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) for inquiry on 21 November 2014. The PJCIS tabled its *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the PJCIS Report) on 27 February 2015.

2. The PJCIS concluded that implementation of a mandatory data retention regime is necessary to maintain the capability of national security and law enforcement agencies and recommended that the Bill be passed (recommendation 39).

3. The PJCIS also recommended that the Bill be amended to strengthen the privacy safeguards and oversight mechanisms contained in the proposed data retention scheme.

4. On 3 March 2015 the Government announced that it would accept all of the Committee's recommendations. The Government will move a number of amendments to the Bill to implement the recommendations made by the PJCIS in its report.

5. These amendments also implement the 'journalist information warrant', which is designed to protect the confidentiality of journalists' sources. The journalist information warrants regime prohibits agencies from making authorisations to access journalists' or their employers' data for the purpose of identifying a confidential source unless a journalist information warrant is in force. The journalist information warrants regime recognises the public interest in protecting journalists' sources while ensuring agencies have the investigative tools necessary to protect the community.

6. The Government will also move amendments to the *Intelligence Services Act 2001*, the *Telecommunications Act 1997*, the *Privacy Act 1988* and the *Australian Security Intelligence Organisation Act 1979* to give effect to recommendations made in the PJCIS Report.

FINANCIAL IMPACT STATEMENT

7. The amendments to the Bill do not have a financial impact.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

Amendments to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

8. 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 Amendments

9. The proposed amendments to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) implement recommendations of the *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* tabled in Parliament on 27 February 2015 (the PJCIS Report). The proposed amendments to the Bill focus primarily on increasing Parliamentary oversight of the proposed mandatory data retention scheme, and on strengthening safeguards, oversight and accountability mechanisms relating to access to telecommunications data more broadly.

10. In response to a recommendation in the PJCIS Report, an amendment to the *Intelligence Services Act 2001* (the ISA) will be made to give the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) the ability to inquire into operational matters relating to the use of telecommunications data by the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) in relation to the AFP's counter-terrorism functions.

11. The amendments also introduce a journalist information warrant regime. Agencies are prohibited from authorising disclosure of a journalists' or their employers' telecommunications data for the purposes of identifying a source of the journalist without a warrant issued from an independent issuing authority.

12. Furthermore, the amendments to the Bill amend the *Telecommunications Act 1997* (the Telecommunications Act), the *Privacy Act 1988* (the Privacy Act) and the *Australian Security Intelligence Organisation Act 1979* to implement recommendations of the PJCIS Report.

Overview of measures

Telecommunications (Interception and Access) Act 1979

13. The proposed amendments to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) implement the Government's response to recommendations from the PJCIS Report and introduce a journalist information warrant scheme. These amendments will:

- include the data set (amended to incorporate the recommendations of the Data Retention Implementation Working Group[1]) in the TIA Act
- clarify that service providers are only required to retain telecommunications data to the extent that such information is, in fact, available to a service provider
- define the term 'infrastructure' in the Bill
- require the Communications Access Co-ordinator (the CAC) to consider the objects of the Privacy Act when considering whether to make a declaration under proposed section 187B(2)
- make declarations in relation to a 'criminal law-enforcement agency', an 'enforcement agency', items in the data set and classes of service providers, however these declarations cease to be in force after 40 sitting days of either House of Parliament after the declaration comes into force
- require that any future Bill that seeks to amend the list of criminal law-enforcement agencies, enforcement agencies, items in the data set or classes of service providers be referred to the PJCIS with a minimum of 15 sitting days to review and report on the Bill
- establish a journalist information warrant scheme which will require ASIO and enforcement agencies to obtain a warrant from an independent issuing authority prior to authorising disclosure of telecommunications data for the purpose of identifying a journalist's source
- require agencies to provide a copy to the Commonwealth Ombudsman or the Inspector-General of Intelligence and Security of each authorisation that authorises disclosure of information for the purpose of determining the identity of a journalist's source
- require all service providers to be compliant, in respect of retained data, with the Privacy Act and Australian Privacy Principles (APPs)
- enable the CAC to refer disputes over proposed implementation plan exemptions or variations to the Australian Communications Media Authority (the ACMA) for determination
- provide that the characteristics of a binding scheme in relation to the protection of personal information referred to in proposed sections 110A(4)(c)(ii) and 176A(4)(c)(ii) include a mechanism:
    - for monitoring the authority or body's compliance with the scheme, and
    - to enable individuals to seek recourse if their personal information is mishandled.

[1] The Implementation Working Group (IWG) is a joint government-industry group which was established by the Government when the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 was introduced into Parliament on 30 October 2014. The IWG is chaired by the Secretary of the AGD, with the Director-General of the Australian Security Intelligence Organisation and the Commissioner of the Australian Federal Police as co-deputy chairs. IWG membership also includes the Secretary of the Department of Communications, the Chief Executive Officer of the Australian Crime Commission, senior executives of Telstra and Optus and the Chief Executive Officer of Communications Alliance, an industry body representing more than 150 Australian telecommunications companies. The role of the IWG is to consult with industry to support the effective implementation of the proposed data retention obligations.

- list the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) as criminal law-enforcement agencies
- prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime
- clarify that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime
- limit the circumstances in which enforcement agencies may access telecommunications data by requiring that an authorised officer, before making an authorisation under Division 4 or 4A of Part 4-1 of the Act, be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate and that the authorised officer have regard to:
    - the gravity of the conduct being investigated, including the seriousness of any criminal offence, pecuniary penalty or protection of the public revenue
    - whether the authorisation is sought for the location of missing persons
    - the reason why the disclosure is proposed to be authorised, and
    - the likely relevance and usefulness of the information or documents to the investigation.
- require the PJCIS to commence its review of the operation of the data retention scheme no later than the second anniversary of the end of the implementation period
- require that the annual report prepared under section 187P include information on the operation of the data retention and the use of journalist information warrants
- include the following information:
    - costs of the mandatory data retention scheme, and
    - use of implementation plans under the mandatory data retention scheme
- require that the annual report prepared under subsection 186(1) on authorisations for the disclosure of telecommunications data include the following information:
    - category of purpose for accessing data, including a breakdown of types of offences
    - age of data sought
    - number of requests for traffic data
    - number of requests for subscriber data,
    - number of journalist information warrants issued, and
    - number of authorisations issued under journalist information warrants.
- require service providers to protect and encrypt telecommunications data that has been retained for the purposes of the mandatory data retention scheme.
- enable the Prime Minister to declare persons to be Public Interest Advocate for the purposes of making submissions to the issuing authority on warrants permitting the making of authorisations to disclosure telecommunications data for the purposes of identifying a journalist's source.

Intelligence Services Act 2001

14. The proposed amendment to the ISA implements the Government's response to recommendation 34 of the PJCIS Report. This amendment grants the PJCIS the ability to inquire into operational matters relating to the use of telecommunications data by ASIO as well as to the AFP in relation to its counter-terrorism functions. The proposed amendments also make consequential changes to the ISA to give effect to the journalist information warrants regime.

Telecommunications Act 1997

15. The proposed amendment to the Telecommunications Act implements the Government's response to recommendation 23 of the PJCIS Report. This amendment prohibits civil litigants from being able to access telecommunications data that is kept by a service provider solely for the purpose of complying with the mandatory data retention regime, and that is used only for that purpose or a limited number of public interest purposes (such as preserving the safety of life at sea). The amendment includes a regulation making power to create appropriate exceptions.

Privacy Act 1988

16. The proposed consequential amendments to the Privacy Act implement recommendations 24 and 35 of the PJCIS Report. These amendments will, respectively, clarify that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime and require all service providers, regardless of their size, to be compliant with the Australian Privacy Principles (APPs), in respect of retained data,.

Australian Security Intelligence Organisation Act 1979

17. The proposed amendments to the ASIO Act give effect to recommendation 33 of the PJCIS Report insofar as it applies to ASIO. Section 94 of the ASIO Act has been amended to ensure that ASIO's classified annual report will include the information requested in recommendation 33 of the PJCIS Report, including the number and purposes of authorisations to access retained data, the lengths of time for which relevant documents covered by the authorisations were held and the number of authorisations that related to subscriber data and traffic data respectively. The Act will also be amended to require ASIO to include the number of journalist information warrants and authorisations made under journalist information warrants to be included in its classified annual report. The proposed amendments also make consequential changes to the ASIO Act to give effect to the journalist information warrants regime.

Human rights implications

18. The amendments to the Bill engage 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 freedom of expression contained in Article 19 of the ICCPR
- the right to an effective remedy contained in Article 2(3) of the ICCPR
- the right to a fair hearing in Article 14 of the ICCPR

19. To the extent that the proposed Government amendments to the Bill do not displace or substantively modify foundational measures contained in the Bill, the rights-based implications of those measures are comprehensively addressed in the Explanatory Memorandum tabled in Parliament on 30 October 2014. An analysis of the human rights engaged by the proposed Government amendments is outlined below.

Implementation of Recommendations from the PJCIS Report

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

20. A number of measures implementing PJCIS recommendations engage 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. For interference with privacy not to be arbitrary it must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. Reasonableness in this context incorporates notions of proportionality to the end sought and necessity in the circumstances.

21. The following amendments to the Bill engage and promote the right to privacy. A number of the proposed Government amendments also serve to enhance privacy protections for individuals by supplementing and augmenting existing oversight and accountability mechanisms contained in the Bill as originally introduced. These measures, which respond to PJCIS recommendations, expand the existing integrated suite of oversight mechanisms and safeguards which apply to the use of and access to telecommunications data:

- Items 1, 12, 15 to 21 and 24 will require service providers to protect and encrypt telecommunications data that has been retained. This requirement will supplement the existing information security obligations under the Privacy Act and the Telecommunications Consumer Protection Code, and adds an additional layer of privacy and security protection for customer data, supporting the confidentiality of that information.
- Items 5, 8, 66 and 74 will provide that any Ministerial declarations made in relation to the data retention scheme cease to have effect 40 sitting days after a declaration comes into force. The amendments will require that any permanent addition to the data set, classes of service providers that must comply with the data retention regime

or list of criminal law-enforcement agencies or enforcement agencies that can access retained data, must be introduced through amendments to the TIA Act. Any such amendments to the TIA Act must then be referred to the PJCIS for inquiry. These provisions ensure that any proposed permanent change to the data retention regime is considered by the Parliament, facilitating further parliamentary scrutiny.

- Item 6 clarifies that service providers are only required to retain telecommunications data to the extent that such information is, in fact, available to that service provider. They are not required to retain information about communications passing 'over the top' of the underlying service they provide, which are being carried by means of another service, operated by another provider.
- Item 8 will place the dataset in primary legislation. This amendment places the detail of the data retention obligation clearly on the face of the legislation, providing certainty and clarity to providers and telecommunications users. The data set is supported by a declaration power (subject to Parliamentary disallowance and Committee scrutiny) so the dataset can be amended where necessary to rapidly respond to advancements in telecommunications technology or the use of telecommunications services. The amendment recognises that the dataset is central to the operation of the proposed data retention regime and provides a high level of certainty for industry and the Australian public that there are adequate safeguards in place to scrutinise any amendments to the dataset. This amendment also accords with the Parliamentary Joint Committee on Human Rights recommendation 1.36 in its Report into the Examination of legislation in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011*[2]that the Bill be amended to define the types of data to be retained to avoid arbitrary interference with the right to privacy that may result from specifying types of data to be retained in regulations.
- Items 9, 10 and 11 amend section 187B to require the CAC to consider the objects of the Privacy Act when considering whether to make a declaration to apply the data retention obligation to additional services under proposed subsection 187B(2); require the CAC to consult with the Australian Privacy Commissioner before making a declaration if there is any uncertainty or a need for clarification, require the CAC to consider any submissions made by the Australian Privacy Commissioner as a result of such consultation, and require the CAC to notify the PJCIS of any declaration made under 187B(2) as soon as practicable after it is made. This measure enhances existing privacy protections by requiring that the CAC have regard to applicable privacy considerations and ensures that the Privacy Commissioner is consulted where necessary as part of the CAC's deliberations.
- Item 29 amends Schedule 1 to make it clear that individuals have the right to access their personal telecommunications data retained by a service provider under the data retention regime. This amendment is consistent with existing policy for access to personal information under the Privacy Act and reinforces existing individual rights

[2] Fifteenth Report of the 44th Parliament scrutinising Bills introduced 20-30 October 2014 (November 2014) at 14

to obtain access to, correct and annotate personal information provided by the Privacy Act.

- Item 46 increases the threshold requirement in section 180F for authorisations to disclose telecommunications data to require that the authorising officer be 'satisfied on reasonable grounds' that a particular disclosure or use of telecommunications data being proposed is proportionate to the intrusion into privacy (as opposed to "having regard to whether any interference with privacy is justifiable"). This item also requires the authorising officer to have regard to a number of specified factors, including the gravity of the conduct being investigated, the reason why the disclosure is proposed to be authorised and the likely relevance and usefulness of the information to the investigation. This measure will bolster privacy safeguards by ensuring agencies weigh the proportionality of the intrusion into privacy against the value of the evidence and the assistance to be provided to the investigation.
- Items 65 and 73 will require that the characteristics of a binding scheme in relation to the protection of personal information referred to in proposed subparagraph 110A(c)(ii) of the TIA Act include a mechanism for monitoring the authority or body's compliance with the scheme and enable individuals to seek recourse if their personal information is mishandled. This measure ensures a greater level of protection of personal information where an enforcement agency is not subject to the protections afforded by the Privacy Act, or a binding scheme that provides a comparable level of privacy protection.

22. In summary, the above measures promote the right to privacy by enhancing privacy protections through, for example, additional Parliamentary disallowance provisions, directly linking Privacy Act protections, appropriate oversight by the Privacy Commissioner and PJCIS scrutiny.

Right to an effective remedy

23. Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights or freedoms recognised by the ICCPR, including the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the State.

24. Item 25 will amend the Bill to allow for the CAC to refer disputes over applications for exemptions from and variations to data retention obligations to the Australian Communications Media Authority (the ACMA).

25. Item 25 engages and promotes the right to an effective remedy because it will provide service providers with an additional remedial avenue for the resolution of disputes by the ACMA in relation to exemptions or variation decisions made by the CAC.

26. The Bill currently confers on ACMA a role to arbitrate disputes in relation to data implementation plans between the CAC and service providers. However, there is no referral

power to facilitate review by the ACMA when a service provider has applied to the CAC for an exemption or variation from the data retention obligations. This amendment will implement recommendation 15 of the PJCIS Report.

27. The amendment will allow the ACMA to review decisions relating to exemptions from or variations to data retention obligations. This amendment engages and promotes the right to an effective remedy for administrative decision making by providing further review by the ACMA of exemption and variation decisions.

28. Providing further administrative review of CAC decisions, in addition to judicial review[3], advances an applicant's right to an effective remedy.

Right to a fair hearing

29. Article 14(1) of the ICCPR provides that all persons shall be equal before the courts and tribunals and that, in the determination of an individual's rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. This includes respect for the principle of 'equality of arms', which requires that all parties to a proceeding must have a reasonable opportunity of presenting their case under conditions that do not disadvantage them as against other parties to the proceedings.

30. Items 39 and 40 strictly limit the circumstances in which a service provider may disclose data that has been retained for the purpose of Part 5-1A in relation to or as part of civil litigation. This measure engages the right to a fair hearing, specifically the principle of equality of arms because it has the potential to affect procedural fairness in terms of the general conduct of the proceedings and the nature and quantum of evidence capable of being adduced by the parties and available for the court's deliberative processes.

31. Specifically, items 39 and 40 will amend sections 280 and 281 of the Telecommunications Act to limit the disclosure of information or documents kept by a service provider solely for the purpose of complying with Part 5-1A of the TIA Act, and that is used by the service provider only for that purpose, a limited range of public interest purposes (which include using or disclosing data in connection with an emergency warning, a call to an emergency services number, a threat to life situation, or the preservation of human life at sea), or a purpose incidental to those purposes. These items give effect to recommendation 23 of the PJCIS Report. The Committee received evidence of concerns about a possible increase in the frequency and volume of telecommunications data accessed by civil litigants as a result of the implementation of the proposed data retention scheme and the public interest in confining disclosure of and access to, telecommunications data, to protect the broader privacy interests of the community.

[3] Judicial review remains available for decisions made under the TIA Act pursuant to paragraph 75(v) of the Constitution and s 39B of the *Judiciary Act 1901* (Cth))

32. Items 39 and 40 engage Article 14(1) to the extent that prohibiting litigants from accessing telecommunications data as an evidentiary source in civil proceedings could potentially reduce the ability of parties to litigation to access a probative source of information relevant to their claim or response. This has the propensity to affect their legitimate rights and interests in the conduct of civil litigation and constitute an additional *ex ante* barrier to mounting or defending a claim.

33. However, items 39 and 40 do not offend the equality of arms principle as telecommunications data will not be available as an evidentiary source for either party. As such, neither litigant is at a procedural disadvantage in terms or access to evidence or resources to formulate their case. Precluding parties' access to a new source of information does not purport to, nor effectively regulate, the rules of evidence in courts and tribunals or impact the way in which other sources of evidence are collected or presented by either party. The amendments seek to ensure that access to data that is currently available to claimants and respondents is not reduced or limited, as the prohibition is limited to data held solely for the purposes of compliance with the new data retention obligation and related purposes.

34. Items 39 and 40 also contain a regulation making power permitting the Minister administering the Telecommunications Act to prescribe exceptions to this prohibition. This will enable exceptions to be formulated with the benefit of, and informed by, detailed empirical information about the use and application of telecommunications data in civil proceedings and enable any anticipated practical impediments to the conduct of litigation to be appropriately addressed. The prohibition on the disclosure of retained data in connection with civil proceedings will not commence until the proposed data retention scheme is implemented, ensuring the Government has sufficient time to identify and put in place appropriate exceptions.

35. In summary, none of the fundamental tenets of the right to a fair hearing, including the equality of arms principle are removed, compromised or reduced by the proposed measure. Although the right to a fair hearing is potentially engaged by this measure, it is not limited, in that it would not undermine or compromise the overall procedural efficacy of civil proceedings. The ability of an applicant or plaintiff to present their case or to challenge the case against them is not compromised as the restriction on access to telecommunications data applies equally to both parties. As a result, this measure will not prevent one party accessing their opponent's submissions, nor will it compromise procedural equality or generally restrict access to admissible evidence relied on by the other party or adduced in the proceedings.

Journalist information warrant regime

36. As outlined above, Article 17 of the ICCPR provides that everyone has the right to freedom from unlawful or arbitrary interferences with their privacy (the right to privacy). Article 19(2) of the ICCPR provides that everyone has the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds,

regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media. A journalist's right to protect confidential information derives from the right to freedom of expression and is a fundamental tenet of an open and unimpeded press. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the ability of the press to provide accurate and reliable information may be adversely affected.

37. Item 47 of the Bill promotes the right to freedom of expression and the right to privacy in that it provides a higher threshold for the authorisation of disclosures of telecommunications data for the purposes of identifying a journalist's source.

38. Specifically, item 47 will create a scheme that will require ASIO and enforcement agencies to obtain a warrant prior to authorising the disclosure of telecommunications data to identify a journalist's source. The effect of item 47 is to prohibit enforcement agencies from making historic or prospective data authorisations for access to a journalist's or their employer's data for the purpose of identifying a confidential source unless a journalist information warrant is in force that authorises the making of such authorisations.

39. In effect, agencies will be required to obtain a journalist information warrant relating to an investigation into a particular journalist from an independent issuing authority, or, in the case of ASIO, the Minister, as a condition precedent to the agency being permitted to authorise the disclosure of telecommunications data by carriers for that investigation. Notably, the warrant scheme will have the same protections, safeguards and oversights that apply to agencies when they obtain telecommunications interception warrants. The features of the scheme include creating new issuing authorities for the journalist information warrants; use and disclosure offences and exceptions for agencies that obtain data relating to journalists and their sources; allowing Public Interest Advocates, at both the Commonwealth and State and Territory levels, to make submissions to warrant issuing authorities; statistical reporting by enforcement agencies in the public TIA Act Annual Report and by ASIO in its classified Annual Report; and retention of information about the use of these warrants by agencies so that the PJCIS may have access to that information in its long term review of the data retention scheme.

40. Item 43 of the Bill promotes the right of journalists to seek and impart information by introducing specific safeguards to protect the confidentiality of journalists' sources. These protections include achieved high threshold for access through *ex ante* judicial review of a warrant for data authorisation requests ensuring that data access for the purposes of identifying a source receives specific and dedicated independent attention. This measure will ensure that such access is only permitted in circumstances where the public interest in the issue of the warrant outweighs the public interest in maintaining the confidentiality of the source. As a corollary, the item also promotes the corresponding right of the public to receive information disseminated by a journalist in such circumstances, augmenting the ability of the press to provide information on matters of public interest. This item further promotes the right to freedom from arbitrary and unlawful interferences with privacy of the

source and the journalist, by providing for stronger protections that will apply where an agency is seeking to access telecommunications data relating to the journalist or their employer for the purpose of identifying the source.

41. Independent oversight, through the creation of a warrant scheme approved by a judicial officer or AAT member minimises the potential for deterring sources from actively assisting the press to inform the public on matters of public interest and ensures that the media is not adversely affected by the measure. The existence of robust oversight of authorisation requests militates against access to source information occurring in a way which is unduly privacy intrusive. Further, consistent and routine scrutiny of authorisations by independent issuing authorities will further assist in building public trust about how law enforcement and intelligence agencies are using or seeking to use coercive powers. Journalists, by extension, will have a greater level of surety that the confidentiality of their sources will be preserved save where the public interest in identification outweighs the interest in confidentiality.

42. The additional protection afforded to these data authorisations complements journalists' limited privilege to not be compelled to identify their sources where they have given an undertaking of confidentiality and is responsive to media concerns centring on press freedom and the protection of journalists' sources. The Court of Justice of the European Union (CJEU), in assessing the former EU Data Retention Directive, observed that '[the Directive] does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.' (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others (Irish Human Rights Commission intervening); In re Kärntner Landesregierung and others* (Joined Cases C-293/12 and C-594/12); [2014] WLR (D) 164). The amendments add a further warrant threshold, providing a significant additional and unique protection in relation to the identification of confidential journalist sources.

43. Further, the statutory criteria to which issuing authorities must have regard in considering a journalist information warrant application, including whether the interest in the disclosure of data outweighs the interest in confidentiality of the source, with particular regard to the impacts on individual privacy, the gravity of the conduct in relation to which the warrant is sought and the potential investigative utility of the information will ensure that privacy and public interest considerations are always taken into account before a journalist information warrant is granted. Issuing authorities, based on their particular experience and qualifications, are well placed to weigh source confidentiality against the operational outcomes sought to be achieved by disclosure.

Conclusion

44. The amendments to the Bill are compatible with human rights because they promote relevant rights and do not impermissibly derogate from human rights.

NOTES ON CLAUSES

Schedule 1 Amendments

Item 1 – Ensuring the confidentiality of information

45. This item inserts the phrase 'in accordance with section 187BA and' into proposed section 187A. This item implements the relevant parts of recommendation 27 of the *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the PJCIS Report).

46. This item requires that service providers comply with new information security and encryption obligations contained in proposed section 187BA in relation to information and documents that service providers are required to keep under proposed section 187A.

Item 2 – Removal of regulation making power for the data set

47. This item replaces the reference to information of a kind 'prescribed by the regulations' in paragraph 187A(1)(a) with a reference to information of a kind referred to in proposed section 187AA. This amendment is consequential to the insertion of the dataset into the primary legislation.

48. The effect of this item is to remove the power to make regulations to specify which types of information or documents that service providers must retain (the data set) in order to comply with their data retention obligations.

49. This item implements recommendation 2 of the PJCIS Report that the Bill be amended to include the proposed data set in primary legislation.

Item 3 – Removal of references to matters in the data set to be prescribed

50. This item amends the Bill by removing proposed subsection 187A(2). Proposed subsection 187A(2) in the Bill provided that the dataset to be prescribed in the regulations had to relate to the matters referred to in the subsection.

51. Item 2 removes the description of information that may be prescribed by regulation in relation to the data set.

52. Item 3 implements recommendation 2 of the PJCIS Report that the Bill be amended to include the proposed data set in primary legislation.

Items 4 and 5 – Declaration of additional classes of service providers to expire after 40 sitting days

53. Item 4 and 5 amend the Bill to permit the Minister to declare additional services to be the subject of the data retention obligation.

54. Subsection 187A(3A) provides the Minister with a power to declare a service to be within the data retention scheme.

55. Subsection 187A(3B) provides that a declaration under subsection 187A(3A) ceases to be in force after 40 sitting days of either House of Parliament after the declaration comes into force. However, such a declaration may be expressed to enter into force either when it is made or at some later date. The time to expiry of the declaration will only commence once the declaration comes into force.

56. Subsection 187A(3C) provides that, where a Bill is introduced into the Parliament to amend the classes of service providers to which data retention obligations apply (i.e., where a bill is introduced that would permanently list an additional class of service provider on the face of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act)), the Bill must be referred to the PJCIS for inquiry. Subsection 187A(3C) requires the PJCIS to be given a minimum of 15 sitting days of a House of the Parliament for review and report on the bill.

57. Items 4 and 5 give effect to recommendation 14 of the PJCIS Report.

Item 6 – 'Over the top' services

58. This item omits paragraph 187A(4)(c) of the Bill and replaces it with a paragraph that provides that a service provider is not required to keep, or cause to be kept information to the extent that it relates to a communication that is being carried by means of another service that is of a kind referred to in paragraph 187A(3)(a) and that is operated by another person using the relevant service operated by the service provider. Furthermore, a service provider is not required to keep, or cause to be kept a document to the extent that it contains such information. This item seeks to ensure that service providers are only required to retain telecommunications data to the extent that such information is available to that service provider.

59. This item also introduces a note at the end of proposed paragraph 187A(4)(c) putting beyond doubt that service providers are not required to keep information or documents about communications that are carried or enabled by means of services that they themselves do not provide that pass 'over the top' of the underlying service they provide. This item implements recommendation 6 of the PJCIS Report.

Item 7 – Removal of subsection 187A(7)

60. This item removes proposed subsection 187A(7) of the Bill, which provided that for the purposes of certain information or documents required to be retained by service providers, two or more communications that together constitute a single communications session are taken to be a single communication.

61. Proposed subsection 187A(7) now appears in substantially the same form in subsection 187AA(6) inserted by item 8.

Item 8 – Information to be kept

62. This item amends the Bill by inserting a proposed section 187AA, which lists the information or documents that service providers must retain in order to comply with their data retention obligations.

63. The effect of item 8 is to prescribe the data set in primary legislation, implementing recommendation 2 of the PJCIS Report.

64. Subsection 187AA(1) sets out the data set that service providers must retain. The table below sets out explanatory material relating to each of the categories of information or documents that service providers must retain for the purposes of this section.

Information or documents to be kept			
Item	**Topic** **Column 1**	**Description of information** **Column 2**	**Explanation**
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: i) any name or address information; ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service or any related account, service or device	This category includes customer identifying details, such as name and address. It also includes contact details, such as phone number and email address. This information allows agencies to confirm a subscriber's identity or link a service or account to a subscriber. This category also includes details about services attached to account, such as the unique identifying number attached to a mobile phone, or the IP address (or addresses) allocated to an internet access account or service. This category further includes billing and payment information. Information about the status of a service can include when an account has been enabled or suspended, a relevant service has been enabled or suspended or is currently roaming, or a telecommunications device has been stolen. The phrases 'any information' and 'any identifiers' should be read to mean the information that the provider obtains or generates that meets the description which follows that phrase. If the provider has no information that meets the description, including because that kind of information does not pertain to the service in question, no information needs to be retained. For instance, if a provider offers a free service and therefore has no billing information, no billing information needs to be retained by that provider with respect to that service the provider will need to retain subscriber and transactional data with respect to that service, but no billing information needs to be retained. Service providers are not required to collect and retain passwords, PINs, secret questions or token codes, which are used for authentication purposes.

Information or documents to be kept			
Item	**Topic** **Column 1**	**Description of information** **Column 2**	**Explanation**
2	The source of a communication	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.	Identifiers for the source of a communication may include, but are not limited to: • the phone number, IMSI, IMEI from which a call or SMS was made • identifying details (such as username, address, number) of the account, service or device from which a text, voice, or multi-media communication was made (examples include email, Voice over IP (VoIP), instant message or video communication) • the IP address and port number allocated to the subscriber or device connected to the internet at the time of the communication, or • any other service or device identifier known to the provider that uniquely identifies the source of the communication. In all instances, the identifiers retained to identify the source of the communication are the ones relevant to, or used in, the operation of the particular service in question.

Information or documents to be kept			
Item	**Topic** **Column 1**	**Description of information** **Column 2**	**Explanation**
3	The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: a) has been sent; or b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.	Paragraph 187A(4)(b) puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history. The destination of a communication is the recipient. Identifiers for the destination of a communication may include, but are not limited to: • the phone number that received a call or SMS • identifying details (such as username, address or number) of the account, service or device which receives a text, voice or multi-media communication (examples include email, VoIP, instant message or video communication) • the IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication, or • any other service or device identifier known to the provider that uniquely identifies the destination of the communication. For internet access services, the Bill explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed. In all instances, the identifiers retained to identify the destination of the communications are the ones relevant to, or used in, the operation of the particular service in question. If the ultimate destination of a communication is not feasibly available to the provider of the service, the provider must retain only the last destination knowable to the provider.

Information or documents to be kept			
Item	**Topic** **Column 1**	**Description of information** **Column 2**	**Explanation**
4	The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): a) the start of the communication b) the end of the communication c) the connection to the relevant service, and d) the disconnection from the relevant service.	For phone calls this is simply the time a call started and ended. For internet sessions this is when a device or account connects to a data network and ends when it disconnected – those events may be a few hours to several days, weeks, or longer apart, depending on the design and operation of the service in question.
5	The type of a communication and relevant service used in connection with a communication	The following: a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. c) the features of the relevant service that were, or would have been, used by or enable for the communication. Examples: call waiting, call forwarding, data volume usage.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service (5(b)) provides more technical detail about the service. For example, for a mobile messaging service, whether it is an SMS or MMS. Data volume usage, applicable to internet access services, refers to the amount of data uploaded and downloaded by the subscriber. This information can be measured for each session, or in a way applicable to the operation and billing of the service in question, such as per day or per month. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).

Information or documents to be kept			
Item	**Topic** **Column 1**	**Description of information** **Column 2**	**Explanation**
6	the location of equipment or a line used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: a) the location of the equipment or line at the start of the communication; b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.	Location records will be limited to the location of a device at the start and end of a communication, such as a phone call or Short Message Service (SMS) message. For services provided to a fixed location, such as an ADSL service, this requirement can be met with the retention of the subscriber's address. Paragraph 187A(4)(e) of the Bill provides that location records are limited to information that is used by a service provider in relation to the relevant service. This would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication. Service providers will not be required to keep continuous, real-time or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the locations records to be kept by service providers will not allow continuous monitoring or tracking of devices.

65. Subsection 187AA(2) permits the Minister the power to make a declaration to modify the data set provided for in subsection 187AA(1). Subsection 187AA(2) is subject to subsections 187AA(3)-(4), which set out when such a declaration will be in force and the Minister's powers in relation to the declarations.

66. Subsections 187AA(2)-(5) implement Recommendation 3 of the PJCIS Report.

67. Subsection 187AA(2) allows the Minister to amend the dataset on a temporary basis by issuing a declaration. This is designed to cover a situation in which future technologies or changing telecommunications practices require amendments to the data set to ensure the data retention scheme continues to meet its underlying purpose.

68. Paragraph 187AA(3)(a) provides that the declaration will come into force either when it is made or on a later day specified in the declaration. Paragraph 187AA(3)(b) provides that the declaration ceases to be in force after 40 sitting days of either House of Parliament after the declaration comes into force. The time to expiry of the declaration will only commence once the declaration comes into force (which may be later than when it is made).

69. Subsection 187AA(4) requires that when a bill is introduced into either House of Parliament to permanently amend the data set, or any of the limitations on the data set. In those circumstances, the Minister must refer the amendment to the PJCIS and give the PJCIS at least 15 sitting days of a House of Parliament to conduct its review and issue its report.

70. Subsection 187AA(5) provides that, in relation to the telecommunications data required to be retained in items 2,3, 4 and 6 in the dataset in subsection 187AA(1), two or more communications that together constitute a single communications session are taken to be a single communication. This provision is substantially the same as proposed subsection 187A(7) in the Bill, which is removed by item 7.

71. Subsection 187AA(5) ensures 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. 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 of mobile internet access services will only be required to record prescribed location information for the overall communication rather than its constituent components.

72. 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 automatically seek and receive updates.

Item 9 – The Communications Access Coordinator may consult with the Privacy Commissioner

73. This item introduces subsection 187B(2A) which enables the Communications Access Co-ordinator (the CAC) to consult the Privacy Commissioner before making a declaration that data retention obligations apply to an otherwise exempt relevant service.

74. This item implements recommendation 13 of the PJCIS Report by enabling the CAC to consult with the Privacy Commissioner where there is uncertainty or a need for clarification before a declaration is made.

Item 10 – Privacy considerations for the Communications Access Co-ordinator

75. This item introduces paragraphs 187B(3)(ba) and (bb) which require the CAC to have regard to the objects of the *Privacy Act 1988* (the Privacy Act) and any submissions made by the Privacy Commissioner as a result of consultations under proposed subsection 187B(2A) when considering whether to make a declaration.

76. This item implements recommendation 13 of the PJCIS Report by requiring the CAC to consider the objects of the Privacy Act when considering whether to make a declaration under proposed subsection 187B(2) that the data retention obligation applies to an otherwise exempt relevant service.

Item 11 – Communications Access Co-ordinator to give written notice of declaration

77. This item introduces subsections 187B(6) and (7), which requires the CAC to give written notice of a declaration to the Minister (under subsection (6)) who will in turn give the written notice to the PJCIS (under subsection (7)) as soon as practicable.

78. This item implements recommendation 13 of the PJCIS Report by requiring the CAC to notify the PJCIS of any declaration made under section 187B(2) that the data retention obligation applies to an otherwise exempt relevant service as soon as practicable after it is made.

Item 12 – Ensuring the confidentiality of information

79. This item amends the Bill by inserting proposed section 187BA. This item gives effect to recommendation 37 of the PJCIS Report.

80. This item supplements the obligations of service providers under Australian Privacy Principle (APP) 11.1 to 'take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss; and from unauthorised access, modification or disclosure.' Item 29 amends the Bill to provide that the Privacy Act applies to all service providers to the extent that the service provider's activities relate to retained data. Further, item 29 will provide that information and documents kept by a service provider in complying with proposed Part 5-1A are personal information within the meaning of the Privacy Act, and so must be protected in accordance with APP 11.1. This item also supplements the obligations of carriage service providers under clause 4.6.3 of the Telecommunications Consumer Protection Code (C628:2012) to 'have robust procedures to keep its Customers' Personal Information in its possession secure and restrict access to personnel who are authorised by the Supplier.'

81. This item requires service providers to protect the confidentiality of information or documents kept in accordance with proposed section 187A. Service providers are required to protect these records in two ways: by encrypting the information, and by protecting the information from unauthorised interference or unauthorised access.

82. This item does not prescribe a particular type of encryption; the decision about how to implement the encryption required by this proposed item will be a matter for the service provider to determine, in light of all the circumstances including, in particular, the technical configuration of the system or systems used to keep information required to be retained under proposed section 187A, and whether a particular method or set of methods of encryption will be adequate to protect the confidentiality of that information.

83. Where a service provider encrypts retained data, the service provider must retain the technical capability to decrypt and disclose relevant retained data in a useable form in accordance with a lawful request or requirement under the TIA Act or Telecommunications Act.

84. Service providers must also put in place measures that protect against unauthorised interference or access to information retained in accordance with proposed section 187A. However, this item does not prescribe particular measures that must be put in place to afford such protection; the decision about how to implement the protections required by this proposed paragraph will be a matter for the service provider to determine in light of all the circumstances, including in particular the technical configuration of the system or systems used to keep information required to be retained under proposed section 187A, and whether a particular measure or set of measures will be adequate to protect the confidentiality of that information.

85. Under proposed Division 2 of Part 5-1A, as amended by items 12-19, a service provider may seek approval of a data retention implementation plan that replaces the service provider's obligations under proposed section 187BA while the plan is in force. Additionally, under proposed Division 3 of Part 5-1A, as amended by item 24, a service provider may apply for and receive an exemption from or variation to the service provider's obligations under proposed section 187BA. An example of a situation in which such an exemption or variation might be appropriate would be where the cost of encrypting a legacy system that was not designed to be encrypted would be unduly onerous and the service provider has identified alternative information security measures that could be implemented. An exemption however would not normally be appropriate where fulfilling the data protection obligations would be merely inconvenient.

Item 13 – Period for keeping information or documents

86. This item amends the Bill by removing the reference to paragraph 187A(2)(a) in paragraph 187C(1)(a),which prescribes the period for which data must be kept, and substituting a reference to paragraphs (a) and (b) in column 2 of item 1 of the table in subsection 187AA(1).

87. This amendment is consequential on the insertion of the data set into the primary legislation by item 8.

88. The effect of this item will be to provide that, where information or documents relate to subscriber information specified in item 1 of the table in subsection 187AA(1), service providers must keep the information or documents from when they were created until two years after the closure of the relevant account.

89. The purpose of paragraph 187C(1)(a) is to ensure, subject to the amendments made by item 14, that subscriber records specified in paragraphs (a) and (b) of column 2 of item 1 of the table 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 necessary information is available to establish a connection between communications data to be retained and the subscriber to the communications service.

Item 14 - Period for keeping information or documents

90. This item amends the Bill by removing the reference to paragraph 187A(2)(a) in subsection 187C(2) and substituting a reference to paragraphs (a) and (b) in column 2 of item 1 of the table in subsection 187AA(1).

91. This amendment is consequential on the deletion of subsection 187A(2) by item 3 and the insertion of the data set into the primary legislation by item 8.

92. The effect of this item is to provide that regulations can prescribe that certain subscriber information specified in paragraphs (a) and (b) of column 2 of item 1 of the table in subsection 187AA(1) is only required to be retained for a period of two years after it comes into existence, rather than for the period commencing when it comes into existence and expiring two years after the closure of the relevant account.

Item 15 – Ensuring the confidentiality of information

93. This item amends the Bill by inserting a reference to proposed section 187BA, which imposes information protection obligations in relation to retained data into proposed section 187D. This item implements the relevant parts of recommendation 37 of the PJCIS Report in relation to the encryption of retained data.

94. The effect of this item is that, while an approved data retention implementation plan is in force, it has the effect of replacing a service provider's obligations in relation to the protection of retained data with information security obligations set out in the approved plan. These obligations may, but would not necessarily, differ from the obligations set out in proposed section 187BA.

Items 16, 17, 18 and 19 – Ensuring the confidentiality of information

95. These items amend the Bill by inserting references to proposed section 187BA in relation to the protection of retained data into proposed section 187E, which permits a provider to seek approval of a data retention implementation plan. These items implement the relevant parts of recommendation 37 of the PJCIS Report.

96. The effect of these items is to require a service provider that is applying for approval of a data retention implementation plan under proposed section 187E to specify its current information security practices, details of the interim information security arrangements the provider proposes to implement under the plan if approved, and the day by which the service provider will comply with the obligations under proposed section 187BA.

Items 20 and 21 – Ensuring the confidentiality of information

97. These items amend the Bill by inserting references to proposed section 187BA in relation to the protection of retained data into proposed section 187F of the Bill which governs the CAC's consideration of implementation plan applications. These items implement the relevant parts of recommendation 37 of the PJCIS Report.

98. The effect of these items is to require the CAC to consider *inter alia* the desirability of a service provider achieving substantial compliance with its information security obligations in relation to retained data under proposed section 187BA as soon as practicable and the extent to which the plan would reduce the regulatory burden imposed on the service provider under proposed Part 5-1A, including proposed section 187BA.

99. Where, at the time of applying for approval of a data retention implementation plan, a service provider is not compliant with proposed section 187BA, the CAC will be required to consider the reasons for the non-compliance. Reasons for non-compliance that may weigh in favour of the plan being approved, or being given back to the service provider with only minor requests for amendment, may include, for example, that the service provider has made its application shortly after the commencement of proposed section information security obligations and so has not yet modified its existing systems to achieve full compliance, or that a service offered by the service provider has only recently become subject to Part 5-1A, for example as the result of the service being acquired or modified such that it is now a 'relevant service'.

Item 22 – Technical correction

100. This item amends proposed subsection 187H(2) by omitting 'the end of.' This item corrects an error in drafting.

Item 23 – Technical correction

101. This item amends proposed paragraph 187K(3)(b) by substituting 'exemption' with 'decision.' This item corrects an error in drafting.

Item 24 – Ensuring the confidentiality of information

102. This item amends the Bill by inserting a reference to the information security obligations under proposed section 187BA into proposed section 187K. This item implements the relevant parts of recommendation 37 of the PJCIS Report.

103. Proposed section 187K will empower the CAC to exempt or vary the obligations to which a service provider is subject under proposed Part 5-1A of the TIA Act, including the information security obligations under proposed section 187BA. This item amends proposed paragraph 187K(7)(e) to require the CAC, before making a decision about such an exemption or variation, to take into account any alternative information security arrangements that the service provider has identified. This provision acknowledges that encryption, in particular, will not always be the most appropriate information security measure, especially in relation to legacy systems that were not designed to be encrypted. The purpose of this provision is to ensure that the CAC is able to consider alternative information security arrangements that a service provider has identified as being appropriate to implement when considering whether to partially exempt, or to vary, a service provider's information security obligations under proposed section 187BA.

Item 25 – Review of exemption or variation decisions by the ACMA

104. This item amends the Bill by inserting proposed section 187KA, implementing recommendation 15 of the Report of the PJCIS.

105. Under the Bill, the ACMA will have the ability to determine disputes in relation to applications for data retention implementation plans (including applications for amendment). This item will provide the ACMA with the additional role to determine disputes when a service provider has applied to the CAC for an exemption or variation from the data retention obligations. As such, this amendment to the Bill will ensure a consistent approach to disputes between the CAC and service providers regarding the application of data retention obligations.

Item 26 – Capital contribution

106. This item amends the Bill by inserting proposed section 187KB. This amendment is consistent with recommendation 16 of the PJCIS report on the Bill.

107. Proposed section 187KB will provide legislative authority for the Commonwealth to grant financial assistance to service providers to assist them to comply with obligations imposed by the data retention scheme. The terms and conditions of the financial assistance are to be set out in agreements entered into with service providers by the Minister on behalf of the Commonwealth. The financial assistance is to be provided out of money appropriated by the Parliament.

Item 27 – Applications to be kept confidential

108. Item 27 amends the Bill by inserting a proposed subsection 187L(1A). Proposed subsection 187L(1A) requires ACMA to keep confidential any application by a service provider for a review that it receives under subsection 187KA(1). The ACMA will be unable to disclose the service provider's application without the written permission of the service provider.

109. However, this confidentiality requirement does not prevent ACMA providing the application to the CAC and relevant enforcement agencies and security authorities, as subsection 187KA(3) requires the ACMA to provide those agencies or authorities with a copy of the application. This ensures that those agencies and authorities are appropriately consulted.

110. A service provider's application for a review will include details about specific business processes, such as technical network infrastructure specifications which may be commercially sensitive. The obligation on the ACMA, as well as any agencies or authorities 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 security perspective.

Item 28 – Applications to be kept confidential

111. Item 28 amends the Bill by substituting new confidentiality requirements in subsection 187L(2) of the Bill. Item 28 will require the ACMA, the CAC and any enforcement agency or security authority to keep confidential any copy it receives of a service provider's application for:

- approval of a data retention implementation plan
- exemption from or variation of data retention obligations
- review of a CAC decision in relation to exemption or variation of data retention obligations.

112. The principal purpose of this item is to ensure that the CAC and any enforcement agencies or security authorities keep confidential copies of exemption review applications they receive from the ACMA under section 187KA(3).

113. This item also substitutes a reference in the current subsection 187L(2) of the Bill to 'paragraph 187G(1)(a)' with a reference to 'subsection 187G(1)'. This is a technical correction to ensure that the ACMA is required to keep confidential copies of data retention implementation plan applications it receives from the CAC under subsection 187G(1). (The ACMA receives such copies under subsection 187G(1), rather than paragraph 187G(1)(a)). Enforcement agencies and security authorities will continue to be required to keep copies of such applications they receive under subsection 187G(1) confidential.

Item 29 – Application of the Privacy Act

114. This item amends the Bill by inserting a new proposed section 187LA. This item, in conjunction with items 37 and 38, implements recommendations 24 and 35 of the PJCIS Report.

115. Proposed subsection 187LA(1) provides that the Privacy Act applies in relation to a service provider to the extent that the activities of the service provider relate to retained data. The effect of this provision is that the Privacy Act and the Australian Privacy Principles

(APPs) will apply to all service providers as though they were 'organisations', including service providers that would otherwise be exempt from the Privacy Act under the 'small business operator', 'registered political party', 'agency', 'State or Territory authority' or 'prescribed instrumentality of a State or Territory' exemptions contained in section 6C of the Privacy Act. However, this provision applies only to the extent that the activities of the service provider relate to retained data (including, for example, the collection, storage, use, disclosure, including cross-border disclosure, individual access, de-identification and destruction of retained data).

116. Proposed subsection 187LA(2) provides that information or documents kept under proposed Part 5-1A are taken to be 'personal information', within the meaning of the Privacy Act, relating to an individual if the information relates to the individual, or to a communication to which the individual is or was a party. Under the standard definition of personal information, what constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances. As a result, not all information held by service providers may fall within the standard definition of personal information. This item expands the definition of personal information, ensuring that all retained data kept by service providers in accordance with Part 5-1A is personal information within the meaning of the Privacy Act.

117. As a result of proposed section 187LA, individuals will be able to request access to their personal retained data in accordance with APP 12, removing uncertainty about whether particular types of retained data are personal information. This right of access will continue to be subject to the Privacy Act and APPs. In particular, service providers will be able to charge an individual for giving access, in accordance with APP 12.8, and where an individual requests access to information about communications to which they were a party, that information will generally also be the personal information of at least one other individual (being the other party to the communication).

118. Regarding cost recovery in civil litigation proceedings, service providers will be able to apply for reimbursement once they have been served with a subpoena to produce evidence. In civil litigation proceedings, cost recovery is subject to the relevant court rules and procedures, as for example section 15A.10, of the Federal Circuit Court Rules 2001. Service providers will also be required to comply with the information security obligations contained in APP 11.1 in relation to all retained data, and will be required to de-identify or destroy retained data at the expiry of the retention period, unless one of the circumstances in paragraphs b, c or d of APP 11.2 applies.

Items 30 – Review of operation of Part 5-1A of the TIA Act

119. Item 30 amends the Bill by omitting subsection 187N(1) and substituting proposed subsection 187N(1).

120. Subsection 187N requires the PJCIS to review the data retention regime as soon as possible after the third anniversary of the end of the implementation phase. The PJCIS recommended that the commencement date for the review be reduced from three years to two. The PJCIS also recommended that its report on the review be presented to Parliament no later than three years after the end of the implementation period.

121. Item 30 implements recommendation 30 of the PJCIS Report, specifying that the review must start on or before the second anniversary of the end of the implementation phase and finish on or before the third anniversary of the end of the implementation phase.

Item 31 – Record-keeping for review of operation of Part 5-1A of the TIA Act

122. Item 31 inserts subsections 187N(3), (4) and (5) to require the head of an agency to keep, until the PJCIS review of the data retention scheme is completed, a copy of all authorisations made under Chapter 4 of the TIA Act, a copy of all journalist information warrants (and authorisations made under those warrants) made under Chapter 4 of the TIA Act, as well as information reported each year to the Minister relating to the agency's access to historic telecommunications data. This will ensure that the PJCIS review of the data retention scheme in proposed section 187N will have access to comprehensive information held by agencies on their access to telecommunications data.

123. This item implements recommendation 31 of the PJCIS Report that agencies be required to collect and retain information necessary to inform the Committee's review of the data retention scheme.

Item 32 – Annual reports

124. Item 32 inserts proposed subsection 187P(1A). This item implements recommendation 33 of the PJCIS report by requiring that the Annual Report prepared under proposed subsection 187P(1) contain information on the costs incurred by service providers in complying with their proposed obligations, and the use of data retention implementation plans.

Items 33 and 34 – Amendments to the ASIO Act

125. Items 33 and 34 insert amending items 1A-1D in Schedule 1 to the Bill. These items will amend the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to implement the Government's response to PJCIS recommendation 33, insofar as it applies to ASIO, that annual reports on the data retention scheme should cover certain matters. These relate to: the number and types of purposes of authorisations to access retained data; lengths of time for which relevant documents covered by the authorisations were held; and the number of authorisations that related to subscriber data and communications traffic data respectively.

126. Amending items 1A-1D amend the reporting requirements in subsection 94(2A) of the ASIO Act, to ensure that these matters are included in ASIO's annual reports, in relation to ASIO's telecommunications data access. Subsection 94(2A) will be amended to include the number of journalist information warrants issued during the reporting period and the number of authorisations made under those journalist information warrants. Annual reports including this information are subject to Minister's discretion under subsection 94(5) to make deletions from the report to be tabled in Parliament, in accordance with subsection 94(4), in order to avoid prejudice to security, defence, international affairs or the privacy of individuals. The Inspector-General of Intelligence and Security (IGIS) can request classified annual reports in accordance with the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act).

Item 35 and 36 – Amendments to Intelligence Services Act 2001

127. Amendments 35 and 36 insert amending items 1E-1G in Schedule 1 to the Bill. These items will amend the *Intelligence Services Act 2001* (the ISA), principally to implement the Government's response to recommendation 34 of the PJCIS advisory report on the Bill. The PJCIS recommended it be conferred a new statutory function in section 29 of the ISA, enabling it to conduct inquiries into the purpose and manner of access of retained data by ASIO and AFP, arising from relevant annual reports made on the data retention scheme. This includes where this goes to a review of operational matters.

128. Subsection 29(3) of the ISA reflects that it is not a function of the PJCIS to examine operational matters (or matters beyond those pertaining to intelligence and security). That existing provision reflects a principle that operational oversight of Australia's intelligence, security and law enforcement agencies is conducted principally by independent statutory bodies – including the IGIS and the Ombudsman – which report to the relevant responsible Minister.

129. Consistent with this division of responsibilities, amending items 1E-1G will confer upon the PJCIS a new function to conduct a review of the overall effectiveness of the operation of the data retention scheme, in relation to the activities of ASIO and the AFP (in relation to AFP investigations under Part 5.3 of the *Criminal Code 1995*), where those activities are the subject of the relevant annual reporting requirements applying to ASIO and the AFP under the ASIO Act and TIA Act respectively. The PJCIS will be able to inquire into operational matters concerning the relevant data access activities of ASIO (covered in their annual report) and the AFP (covered in the TIA Act annual report)to the extent that such operations are relevant to the Committee's overall assessment of the effectiveness of the data retention scheme in proposed Part 5-1A of the TIA Act.

130. Amending item 1E will insert definitions of new terms in section 3 of the ISA ('retained data activity', and 'service provider') which are used in the provisions of section 29 conferring the PJCIS's new function.

131. Amending item 1F will insert new paragraphs 29(1)(bc), (bd) and (be). New paragraph 29(1)(bc) makes explicit that it is a statutory function of the PJCIS to conduct its review of the data retention scheme under proposed s 187N of the TIA Act, following completion of the implementation phase. New paragraphs 29(1)(bd) and (be) provide, respectively, for the PJCIS's new inquiry function of the data retention activities of ASIO and the AFP (in relation to investigations under Part 5.3 of the *Criminal Code*), in response to PJCIS recommendation 34. The scope of the new inquiry function in paragraph 29(1)(be) in relation to the activities of the AFP (pertaining to Part 5.3 of the *Criminal Code*) is consistent with the PJCIS's existing functions in relation to the AFP under subsection 29(1) of the ISA.

132. Amending item 1G will set out the parameters for the PJCIS's performance of the new function, by inserting proposed subsections 29(4) and 29(5). Proposed subsection 29(4) will provide that the PJCIS can examine matters relating to particular operations of ASIO and the AFP with respect to retained data activities covered in the ASIO annual report and the TIA Act annual report respectively. This is a limited exemption from the prohibitions on inquiring into operational matters in paragraphs 29(3)(c) and 29(3)(k).

133. New paragraph 29(5)(a) provides that the PJCIS's examination of particular operational matters under proposed subsection 29(4) is to be performed for the sole purpose of assessing and making recommendations about the overall operation and effectiveness of the data retention scheme. (New paragraph 29(5)(c) also makes explicit that the new function cannot be performed for any other purpose than that set out in new paragraph (a) of the subsection). These provisions are necessary to preserve the focus of the PJCIS on non-operational matters, and to avoid overlap or duplication with the operational oversight of the IGIS and Ombudsman, while also enabling the PJCIS to access operational information for the purpose of performing its new function.

134. New paragraph 29(5)(b) further qualifies that the new inquiry function is limited to the activities of ASIO and the AFP (in relation to Part 5.3 of the *Criminal Code*), and does not permit reviewing the activities of 'service providers' (as defined in section 3 by reference to that term in the TIA Act). This reflects the intention of the PJCIS in recommendation 34 to facilitate Parliamentary oversight of the purpose and manner of access to retained data by ASIO and the AFP.

135. All of the PJCIS's statutory functions will continue to be governed by the procedural arrangements in Schedule 1 to the ISA. These include the protections for operationally sensitive information (and other information which, if released, would or might prejudice national security or foreign relations) as set out in Parts 1 and 2 of Schedule 1. The Government further intends to work with the PJCIS to develop practical arrangements for the conduct of its new inquiry function. It is anticipated that these working arrangements may address such matters as: the timing of inquiries; strategies for avoiding overlap with extant oversight activities of the IGIS and Ombudsman; and arrangements for requesting, providing and protecting operational and other sensitive information.

Items 37 and 38 – Amendments to the Privacy Act

136. Amending item 1H amends the Privacy Act to insert a note at the end of the definition of 'personal information' contained in subsection 6(1) to draw attention to the extension by the TIA of the meaning of personal information to cover information kept under the data retention scheme.

137. Amending item 1J repeals and replaces the existing explanatory note to the definition of 'organisation' in subsection 6C(1) of the Privacy Act. This note clarifies that under proposed section 187LA service providers are treated as organisations for the purposes of the Privacy Act in relation to the retention of data under Part 5-1A of the TIA Act. Service providers are therefore an 'APP entity' under the Privacy Act and must comply with the APPs in relation to their activities under Part 5-1A of the TIA Act.

Items 39 and 40 – Access to retained data in connection with civil litigation

138. Item 39 and 40 amend the Bill by amending sections 280 and 281 of the Telecommunications Act to give effect to recommendation 23 of the PJCIS Report.

139. Currently, subsection 280(1) of the Telecommunications Act provides that the prohibitions on the disclosure of certain communications-related information and documents under Division 2 of Part 13 of that Act do not apply, other than where the disclosure is in connection with the operation of an enforcement agency within the meaning of the TIA Act, where the disclosure is required or authorised by or under law. Item 39 will insert a new item 3A to Part 2 of Schedule 1 of the Bill that will insert proposed subsections 280(1B) and (1C) to the Telecommunications Act.

140. The effect of proposed subsection 280(1B) will be that paragraph 280(1)(b) does not apply in circumstances where all of the criteria specified in paragraphs 280(1B)(a) to (c) are satisfied. Paragraph 280(1B)(a) will be satisfied where the disclosure is required or authorised because of a subpoena, a notice of disclosure, or an order of a court in connection with a civil proceeding.

141. Telecommunications data that is retained by service providers for their ordinary business purposes or for other regulatory purposes is currently accessed in the course of many civil proceedings. The purpose of proposed paragraph 280(1B)(b) is to ensure that the prohibition applies only to telecommunications data that is collected and retained only for the purpose of complying with proposed Part 5-1A, and that is used by the service provider only for that purpose, a limited range of defined public interest purposes, or for purposes incidental to any of those purposes.

142. An example of a purpose incidental to the purpose listed in proposed subparagraph 280(1B)(c)(i) (complying with proposed Part 5-1A of the TIA Act) would be to develop, test or maintain the systems used to retain data under proposed Part 5-1A. An example of a

purpose incidental to the purposes listed in proposed subparagraphs 280(1B)(c)(ii), (iii) or (iv) (complying with a warrant issued or authorisation made under the TIA Act, or with a request or requirement provided for by sections 284 to 288 of the Telecommunications Act, or a request to provide a person with access to their personal information under the Privacy Act) would be using or disclosing information or documents for the purpose of seeking legal advice in relation to the warrant, authorisation, request or requirement.

143. This provision thereby ensures that telecommunications data that is collected, retained or used for a service provider's ordinary business purposes or other purposes unrelated to the data retention obligation, continues to be available for such proceedings.

144. Proposed paragraph 280(1C)(a) provides that the prohibition contained in proposed subsection 280(1B) does not apply in circumstances of a kind prescribed by the regulations. As noted above, telecommunications data is currently accessed by parties to many civil proceedings, including proceedings relating to international child abduction, family violence, and personal injury or economic harm as a result of negligence or professional malpractice. As the requirement for access will depend substantially on the facts and circumstances of each individual civil proceeding, any limit on the availability of such information would have the potential to prejudice the legitimate rights and interests of claimants or respondents in such proceedings. Therefore, a regulation-making power is required to enable the creation of regulations to prescribe further circumstances for where the prohibition in paragraph 280(1B) would not apply.

145. Proposed paragraph 280(1C)(b) provides that the prohibition contained in proposed subsection 280(1B) does not apply in relation to disclosures to enforcement agencies. A number of enforcement agencies currently obtain access to telecommunications data in the course of civil proceedings such as actions for the proceeds of crime, or in relation to control orders made under Division 104 of the *Criminal Code*.

146. Proposed paragraph 280(1C)(c) provides that the prohibition contained in proposed subsection 280(1B) does not commence until the end of the implementation phase for proposed Part 5-1A of the TIA Act. This provision ensures that the prohibition does not commence until the proposed data retention scheme is implemented.

147. Currently, section 281 of the Telecommunications Act provides that the prohibitions on the disclosure of certain communications-related information and documents under Division 2 of Part 13 of that Act do not apply in relation to a disclosure made by a person of information or a document if the person makes the disclosure as a witness summoned to give evidence or to produce documents.

148. Item 40 will insert a new item 3C to Part 2 of Schedule 1 of the Bill that will insert proposed subsections 281(2) and (3) to the Telecommunications Act. The purpose of these proposed subsections is substantially similar to the purpose of proposed subsections 280(1B) and (1C) of the Telecommunications Act, being to prohibit the disclosure by a witness in civil

proceedings of information or documents that have been kept by a service provider solely for the purpose of complying with proposed Part 5-1A of the TIA Act, and that are not used by the service provider only for that purpose, a limited range of defined public interest purposes, a purpose prescribed by the regulations, or for purpose incidental to the abovementioned purposes.

149. Proposed subsection 281(3) contains exceptions to this prohibition, which are similar to those in proposed subsection 280(1C). In particular, proposed paragraph 281(3)(a) contains a regulation-making power , which has the same purpose as the regulation-making power that would be established by proposed paragraph 280(1C)(a).

Item 41 – Definitions

Definition of 'Defence Minister'

150. This item inserts a definition of 'Defence Minister' into subsection 5(1) of the TIA Act. The 'Defence Minister' has the same meaning as given in the *Intelligence Services Act 2001*.

Definition of 'Foreign Affairs Minister'

151. This item inserts a definition of 'Foreign Affairs Minister' into subsection 5(1) of the TIA Act. The 'Foreign Affairs Minister' has the same meaning as given in the *Intelligence Services Act 2001*.

Definition of 'Public Interest Advocate'

152. This item inserts a definition for the term 'Public Interest Advocate' into the newly created section 180X of the Bill. A 'Public Interest Advocate is defined as a person whose appointment is in force under section 180X(1).

Definition of 'Journalist Information warrant'

153. This item inserts a definition for the term 'journalist information warrant' into subsection 5(1) of the TIA Act. A 'journalist information warrant' means a warrant issued under Division 4C of Part 4-1.

Definition of 'IGIS official'

154. This item inserts a definition of the term 'IGIS official' into subsection 5(1) of the TIA Act. An 'IGIS official' has the same meaning as section 4 of the *Australian Security Intelligence Organisation Act 1979.*

Definition of 'implementation phase'

155. This item also inserts a definition of 'implementation phase' by stating it has the meaning given in subsection 187H(2), which states the implementation phase is the period of 18 months starting on the commencement of the data retention obligations.

Definition of 'infrastructure'

156. This item inserts a definition for the term infrastructure into subsection 5(1) of the TIA Act. It defines infrastructure, as it is used in proposed paragraph 187A(3)(c), to mean any line or equipment used to facilitate communications across a telecommunications network.

157. The term infrastructure is used as part of the three limb test in paragraphs 187A(3)(a), (b) and (c) which defines a relevant service. 'Equipment' is defined in section 5 of the Act, which states equipment means any apparatus or equipment used, or intended for use, in or in connection with a telecommunications network, and includes a telecommunications device but does not include a line. Section 5 of the Act, defines 'line' by reference to the definition in the Telecommunications Act. Section 7 of the Telecommunications Act states a line is a wire, cable, optical fibre, tube, conduit, waveguide or other physical medium used, or for use, as a continuous artificial guide for or in connection with carrying communications by means of guided electromagnetic energy.

158. Servers used to operate an 'over the top' service such as VoIP would fall within the definition of infrastructure. However, 'infrastructure' is not intended to include business premises. For example the headquarters of a company, taken in isolation, would not satisfy the definition of 'infrastructure.'

159. Importantly, a piece of equipment or line meeting the definition of infrastructure does not automatically satisfy paragraph 187(3)(c). For instance, a computer used by an employee in a company's headquarters or marketing office is not directly involved in the provision of a relevant service and therefore does not satisfy paragraph 187(3)(c).

160. This item implements recommendation 11 of the PJCIS Report by defining the term 'infrastructure' in greater detail for the purposes of proposed paragraph 187A(3)(c).

Definition of 'Part 4-1 issuing authority'

161. This item inserts a definition for the term 'Part 4-1 issuing authority' into subsection 5(1) of the TIA Act. A 'Part 4-1 issuing authority' is defined as a person whose appointment is in force under section 6DC.

Definition of 'related account, service or device'

162. This item also inserts a definition of 'related account, service or device' in relation to a service to which Part 5-1A applies. This definition is used in proposed section 187AA.

Definition of 'retained data'

163. This item also inserts a definition for 'retained data' which defines it as information, or documents, that a service provider is, or has been, required to keep under Part 5-1A of the TIA Act.

Definition of 'service provider'

164. This item also inserts a definition of 'service provider' by stating it has the meaning given in subsection 187A(1), which provides that it is a person who operates a service to which new Part 5-1A applies.

Definition of 'source'

165. This item inserts a definition of 'source' into subsection 5(1) of the TIA Act to support the journalist information warrant provisions. This definition is expressed not to apply to item 2 of the table in subsection 187AA(1), where source takes on its natural meaning in the context of a telecommunication.

Item 42 – Issuing authorities

166. This item inserts proposed section 6DC into the TIA Act which provides that the Minister responsible for the administration of the TIA Act can, by writing, appoint a judge of the federal court, including a judge of the Federal Court of Australia, Family Court of Australia or a Federal Magistrate, or a magistrate (where those persons have consented in writing to be appointed as an issuing authority) to be an issuing authority for the purposes of issuing a journalist information warrant.

167. The amendment will also allow the Minister to appoint a person who holds an appointment to the Administrative Appeals Tribunal as Deputy President, full-time senior member, part-time senior member or member (including a part-time or full-time member), who is enrolled, and has been enrolled for at least 5 years, as a legal practitioner of a federal court or of the Supreme Court of a State or Territory for the same purpose.

Item 43 – Oversight by the Inspector-General of Intelligence and Security

168. Item 43 amends the Schedule 1, Part 2 of the Bill to insert new amending items 6B and 6C. These amending items amend section 64 of the TIA Act and its heading.

169. The introduction of specific provisions to the TIA Act permitting a person to deal in information in connection with the performance by the IGIS of his or her functions follows the introduction of similarly specific provisions into the ASIO Act by the *National Security Legislation Amendment Act (No. 1) 2014*. In that context, this item seeks to place beyond doubt that a person may deal in the information described in subsection 64(1), and that an IGIS official and another specified person may deal in the information described in subsection 64(2), in connection with the performance by the IGIS of his or her functions.

Item 44 – Authorisations for access to prospective information or documents

170. Item 44 amends section 176 of the TIA Act which relates to prospective data authorisations made by ASIO. Specifically, item 44 replaces the current paragraph 176(5)(b) with two new subparagraphs. Subparagraph 176(5)(b)(i) states that authorisations under section 176 of the TIA Act end as specified in the authorisation which can be no later than the end of the period of 90 days beginning on the day the authorisation is made. Subparagraph 176(5)(b)(ii) provides that if the authorisation is made under a journalist information warrant then the end of the authorisation can be no later than the end of the period specified in section 180N, being the end of the period for which the warrant is in force.

171. In addition, item 44 replaces the current subsection 176(6) in relation to the revocation of an authorisation where the eligible person is satisfied the disclosure is no longer required with an expanded revocation provision requiring revocation of authorisations made under a journalist information warrant where that warrant was revoked, or the Director-General is satisfied the grounds on which the warrant was issued have ceased to exist.

Item 45 – Authorisations for access to prospective information or documents

172. Item 45 amends section 180 of the TIA Act which relates to prospective data authorisations made by criminal law-enforcement agencies. Specifically, item 45 replaces the current paragraph 180(6)(b) with two new subparagraphs. Subparagraph 180(6)(b)(i) states that authorisations under section 180 of the TIA Act end as specified in the authorisation which can be no later than the end of the period of 45 days beginning on the day the authorisation is made. Subparagraph 180(6)(b)(ii) provides that if the authorisation is made under a journalist information warrant then the end of the authorisation can be no later than the end of the period specified in subsection 180U(3), being the end of period for which the warrant is in force.

173. In addition, item 45 replaces the current subsection 180(7) in relation to the revocation of an authorisation where the authorised officer is satisfied the disclosure is no longer required, with an expanded revocation provision requiring revocation of authorisations made under a journalist information warrant where that warrant was revoked.

Item 46 – Authorised officer required to be satisfied that access to telecommunications data is justified and proportionate

174. Amending item 6A amends section 180F of the Act by omitting the requirement that an officer authorising the disclosure of data 'have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable' and inserting a requirement that they 'be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate'.

175. This amending item implements recommendation 25 of the PJCIS Report by requiring the authorised officer making an authorisation under Division 4 or 4A of Part 4-1 of the TIA Act to be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate.

176. Amending item 6B inserts subparagraph 180F(aa) requiring that the authorised officer must have regard to the gravity of any conduct in relation to which the authorisation is sought, including the seriousness of any criminal offence, the seriousness of any pecuniary penalty, the seriousness of any protection of the public revenue and whether the authorisation is sought for the purposes of finding a missing person when determining whether to disclose or authorise the use of communications.

Item 47 – Journalist information warrant

Division 4C

177. Chapter 4 of the TIA Act regulates how national security and law enforcement agencies may access telecommunications data. Item 43 will insert new Division 4C after Part 4-1 of the TIA Act. The provisions to be inserted by this new Part will establish a journalist information warrant (journalist information warrant). This scheme will require ASIO and enforcement agencies to obtain a warrant prior to authorising disclosure of telecommunications data to identify a journalist's source. The effect of Division 4C is to prohibit ASIO and enforcement agencies from making data authorisations for access to a journalist's or their employer's data for the purpose of identifying a confidential source unless a journalist information warrant is in force.

178. The concept of a 'journalist' is intended to replicate the current approach in Division 119 of the *Criminal Code*, as amended by the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*. Subsection 119.2(3)(f) of the *Criminal Code* provides that where a person is working in a professional capacity as a journalist, or is assisting another person working in a professional capacity as a journalist, they are exempted from the general prohibition from entering or remaining in, a declared area. Similarly, an individual is a journalist under Division 4C if they are working as a journalist in a professional capacity. Indicators that a person is acting in a professional capacity include regular employment, adherence to enforceable ethical standards and membership of a professional body.

179. Subdivision 4C-A establishes that national security and law enforcement agencies are required to obtain journalist information warrants. Subdivision 4C-B establishes the procedures for issuing a journalist information warrant to the Organisation. Subdivision 4C-C establishes the procedures for issuing journalist information warrants to enforcement agencies.

Subdivision A – The requirement for journalist information warrants

Proposed section 180G

180. Proposed section 180G provides that an eligible person must not authorise the disclosure of information or documents under Division 3 relating to a particular person without a journalist information warrant. An 'eligible person' is defined under subsections 175(2) and 176(2) of the TIA Act. Section 180G applies if that eligible person knows or reasonably believes that particular person is working in a professional capacity as a journalist or is the employer of a journalist and the purpose of making the authorisation is to identify another person the eligible person reasonably believes to be a source.

Proposed section 180H

181. Proposed subsection 180H(1) provides that an authorised officer of an enforcement agency must not authorise the disclosure of information or documents under section 178, 178A, 179 or 180 relating to a particular person without a journalist information warrant. An 'authorised officer' is defined in subsection 5(1) of the TIA Act.

182. Proposed subsection 180H(2) provides that an authorised officer of the Australian Federal Police must not authorise the disclosure of information or documents under Division 4A (in connection with the enforcement of the criminal law of a foreign country) relating to a journalist for the purpose of identifying a source. A journalist information warrant is not available for this purpose.

Subdivision B – Issuing journalist information warrants to the Organisation

Proposed section 180J

183. Proposed section 180J provides that the Director-General of Security may request that the Minister issue a journalist information warrant in relation to a particular person. This request must specify the facts and other grounds on which the Director-General considers it necessary to issue the warrant.

Proposed section 180K

184. Proposed section 180K provides that the Minister may require the Director-General of Security to provide the Minister, within a specified period, further information in connection with a request under subdivision B. If the Director-General breaches a requirement under

subsection 180K(1) the Minister may refuse to consider the request or refuse to take any further action in relation to that request.

Proposed section 180L

185. Section 180L provides that after considering a request for a journalist information warrant, the Minister must either issue a warrant that authorises the Organisation to make data authorisations in relation to a person who is working in a professional capacity as a journalist or refuse to issue a journalist information warrant.

186. The Minister must not issue a journalist information warrant unless the Minister is satisfied that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source, having regard to specified factors. These include the anticipated privacy interference, the gravity of the matter for which the warrant is sought, the assistance the information to be sought would provide, whether other reasonable methods, if any, that would be effective to obtain the information have been used, any submissions by a Public Interest Advocate on that application and any other relevant matter.

187. Subsection 180L(3) provides that a warrant issued under the section may specify conditions or restrictions relating to making authorisations under the authority of the warrant.

Proposed section 180M

188. Proposed subsection 180M establishes the procedure for the Director-General of Security to issue journalist information warrants in an emergency. Proposed subsection 180M(1) provides that the Director-General may only issue an emergency journalist information warrant if authorised to do so by a Minister listed in subsection 180M(4) or if those Ministers listed in subsection 180M(4) are unavailable. The Director-General may issue a journalist information warrant if a request under section 180J has been made for the issue of such a warrant in relation to the particular person and the Director-General is satisfied that, security will be, or is likely to be, seriously prejudiced if the Organisation does not obtain access to the relevant information or documents before the journalist information warrant is issued and made available to the Minister. The emergency warrant may be issued if, to the knowledge of the Director-General, the Minister has not made a decision under section 180L and the Minister has not refused to issue the relevant journalist information warrant.

189. Proposed subsection 180M(2) provides that the Director-General may not issue a journalist information warrant unless he or she is satisfied as to the matters set out in subsection 180L(2)(a) and (b).

190. Proposed subsection 180M(3) enables a Minister listed in subsection 180M(4) to orally authorise the Director-General to issue a journalist information warrant if they are satisfied of the matters listed in paragraphs 180L(2)(a) and (b).

191. Proposed subsection 180M(4) provides that where the Director-General is satisfied the Minister is unavailable, an oral authorisation may be provided by the Prime Minister, Defence Minister and the Foreign Affairs Minister.

192. Proposed subsection 180M(5) provides that an emergency authorisation may specify conditions or restrictions relating to issuing the journalist information warrant.

193. Proposed subsection 180M(6) requires the Director-General to ensure a written record of the authorisation provided under subsection 180M(3) is made as soon as practicable, but no later than 48 hours, after the authorisation is given.

194. Proposed subsection 180M(7) provides that a journalist information warrant must specify the period for which it remains in force, and this period must not exceed 48 hours. Proposed subsection 180M(3) does not prevent the Minister from revoking the emergency warrant.

195. Proposed subsection 180M(8) provides that the Director-General must provide the Minister with a copy of the warrant and a statement of the grounds on which the warrant was issued, and either a copy or the record made under subsection 180M(6) or, where a journalist information warrant was issued under subparagraph 180M(1)(e)(ii), a summary of the facts of the case justifying the issuing of the warrant..

196. Proposed subsection 180M(9) provides that the Director-General must give a copy of the journalist information warrant to the Inspector-General of Intelligence and Security within 3 business days of issuing such a warrant. Proposed subsection 180M(10) is intended to ensure proposed subsection 180M(5) has effect despite proposed subsection 185D(1).

Proposed section 180N

197. Proposed section 180N provides that a journalist information warrant issued under this Subdivision must specify the period for which it is to remain in force. The specified period must not exceed 6 months.

Proposed section 180P

198. Proposed section 180P provides that the Director-General of Security must take the necessary steps to discontinue the making of authorisations under a journalist information warrant where the Director-General is satisfied that the grounds on which the warrant was issued no longer exist. The Director-General must also advise the Minister, who under proposed section 180L is the issuing authority for the Organisation in relation to journalist information warrants.

199. These requirements will ensure that authorisations do not continue to be made where the grounds that supported the issue of the warrant no longer apply.

Subdivision C – Issuing journalist information warrants to enforcement agencies

Proposed section 180Q

200. Proposed section 180Q limits the persons in an enforcement agency who can apply for a confidential information source identification warrant.

201. Paragraph 180Q(2)(a) provides that in the case of enforcement agencies that are also interception agencies authority to apply for a confidential information source identification warrant is limited to the persons that can apply for an interception warrant under subsection 39(2) of the TIA Act.

202. Paragraph 180Q(2)(b) sets out that where an enforcement agency is not an interception agency, applications must be made by the chief officer of the agency or an officer of the agency in a management level position that has been nominated by the chief officer of the agency to make applications on the agency's behalf. This limitation ensures that the need to apply for a journalist information warrant is considered at an appropriately senior level in an agency.

203. Subsection 180Q(3) gives the chief officers of enforcement agencies the power to nominate, in writing, management level offices or positions in their agency, the occupants of which can apply on behalf of their agency for a journalist information warrant.

204. Subsection 180Q(4) clarifies that nominations made by chief officers under subsection 180Q(3) are not legislative instruments.

205. Subsection 180Q(5) specifies that applications for a journalist information warrant on behalf of an enforcement agency may be made in writing or any other form.

Section 180R

206. Subsection 180R(1) provides that the issuing authority may require the applicant to provide further information in connection with an application for a journalist information warrant.

207. Subsection 180R(2) sets out what happens if the enforcement agency does not provide the information the issuing authority requires under subsection 180R(1). In these circumstances, the issuing authority can refuse to consider the application or to take any action (or any further action) in relation to the application.

208. The purpose of section 180R is to ensure that an issuing authority can require an enforcement agency to make available to the issuing agency all relevant and necessary

information when considering an application for a journalist information warrant. Section 180R also makes it clear the issuing authority is not required to consider or act on such an application if that information is not provided.

Section 180S

209. This item amends the Bill by inserting proposed section 180S concerning oaths and affirmations. Subsection 180S(1) provides that information given by enforcement agencies to the issuing authority in connection with an application for a journalist information warrant must be given on oath or affirmation.

210. Subsection 180S(2) provides that the issuing authority can administer the oath or affirmation, or can authorise another person. The oath or affirmation may be administered in person, by telephone, video call, video link or audio link.

211. The purpose of section 180S is to ensure that information that the enforcement agency gives to the issuing authority in support of an application for a journalist information warrant complies with the requirements of evidence law for witnesses to take an oath or affirmation before giving evidence.

Section 180T

212. Section 180T provides that after considering an application for a journalist information warrant under proposed section 180T, an issuing authority must either issue a warrant that authorises the requesting agency to make data authorisations in relation to a person who is working in a professional capacity as a journalist or refuse to issue a journalist information warrant.

213. The factors that an issuing authority must consider in making a decision are set out in Subsection 180T(2).

214. An issuing authority can only issue a journalist information warrant if he or she is satisfied that the warrant is reasonably necessary to:

- enforce the criminal law; or
- locate a person reported as missing to the Australian Federal Police or a State Police Force; or
- enforce a law that imposes a pecuniary penalty or protects the public revenue; or
- investigate serious offences or an offence against a Commonwealth, State or Territory law punishable by at least a 3 year imprisonment term., and
- the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of journalists' sources.

215. The issuing authority must also be satisfied that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source, having regard to specified factors. These include the anticipated privacy interference,

the gravity of the matter for which the warrant is sought, the assistance the information to be sought would provide, whether other reasonable methods, if any, that would be effective to obtain the information have been used, any submissions by a Public Interest Advocate on that application and any other relevant matter.

Section 180U

216. Proposed section 180U requires journalist information warrants issued under the Subdivision to be made in accordance with a form to be prescribed.

217. Journalist information warrants must be signed by the issuing authority who issues the warrant and be in the prescribed form. Warrants may list any conditions or restrictions that apply to authorisations made under the warrant and must specify the period for which the warrant is in force. Under proposed subsection 180U(3) and proposed section 180V, journalist information warrants can be in force for up to 90 days, commencing the day the warrant is issued.

218. Proposed subsection 180U(4) provides that warrants cannot be extended beyond the period they are in force. This will ensure that any ongoing operational need to investigate the subject of a journalist information warrant is considered afresh by an issuing authority under the criteria set out in proposed section 180U. Proposed subsection 180U(5) clarifies that while a journalist information warrant cannot be extended, a further warrant can be issued under the TIA Act in relation to a person previously the subject of a warrant under the Act.

Proposed section 180V

219. Proposed section 180V provides that a journalist information warrant comes into force when it is issued.

Proposed section 180W

220. Proposed 180W outlines the revocation of a journalist information warrant. Paragraph 180W(1)(a) states that the chief officer may revoke such a warrant at any time. Paragraph 180W(1)(b) provides that the chief officer of an enforcement agency must revoke such a warrant if satisfied that the grounds on which the warrant were issued to the agency have ceased to exist.

Subdivision D – Miscellaneous

Proposed section 180X

221. Section 180X creates the new role of a Public Interest Advocate.

222. The Public Interest Advocate role will consider and evaluate journalist information warrant applications made by the Organisation and law enforcement agencies pursuant to sections 180L and 180T respectively. The Public Interest Advocate will be able to make independent submissions to the Minister in the case of the journalist information warrants made by the Organisation, and to the issuing authority in the case of the law enforcement agencies, on the proposed undertaking in relation to each application (including conditions or restrictions).

223. Subsection 180X(1) permits the Prime Minister to declare a person to be a Public Interest Advocate.

224. Subsection 180X(3) enables regulations to be made relating to the role of the Public Interest Advocate to support the discharge of its independent role. Subsection 180X(4) clarifies that a declaration of an Advocate is not a legislative instrument.

Items 48-50 – Consequential changes to use and disclosure provisions

225. These items amend the Bill to insert new paragraphs into the use and disclosure provisions contained in Part 4-1 Division 6 of the TIA Act. These are consequential amendments relating to the implementation of recommendations 27 and 34 of the PJCIS Report.

226. These items ensure that ASIO, enforcement agencies, IGIS, the Commonwealth Ombudsman, the Minister and the PJCIS are able to use and disclose authorisations made under Chapter 4 of the TIA Act and associated information for the purposes of the new oversight and reporting functions recommended by the PJCIS in its report.

227. The introduction of specific provisions to the TIA Act permitting persons to deal in information for the purpose of the IGIS exercising powers, or performing functions or duties, under the IGIS Act follows the introduction of similarly specific provisions into the ASIO Act by the *National Security Legislation Amendment Act (No. 1) 2014*. In that context, these items seek to place beyond doubt that a person use or disclose the information described in sections 181A and 182 for the purpose of the IGIS exercising powers, or performing functions or duties, under the IGIS Act.

Item 51 – Use and disclosure provisions

228. Item 51 will insert amending item 6V in Schedule 1 to the Bill. This item inserts new sections 182A and 182B in the TIA Act, and relates to the introduction of journalist information warrants.

229. Proposed section 182A creates an offence where a person discloses or uses a journalist information warrant or information about such a warrant. Commission of the offence attracts a penalty of two years imprisonment.

230. Proposed section 182B outlines the circumstances in which disclosures and use are permitted. An enforcement agency may use or disclose such a warrant or information about such a warrant to a third party for the specified purposes set out in the section. Such purposes include enabling the making of submissions under section 180X by a Public Interest Advocate, enabling a person to comply with their notification obligations under section 185D or 185DE in relation to journalist information warrants, enabling ASIO to perform its functions, or to enforce the criminal law, the enforcement of a law imposing a pecuniary penalty, or the protection of the public revenue. In addition, a disclosure to and by an IGIS official (in connection with the exercising of the powers, or performing functions or duties of the IGIS) is permitted.

231. The note following proposed section 182B indicates that where a person is charged in relation to a contravention of new section 182A, the defendant bears an evidential burden to demonstrate that the disclosure or use was lawful.

Item 52 – Retention of authorisations

232. Item 52 amends the Bill to insert subsection 185(3) into the TIA Act. This item ensures that section 185 of the TIA Act does not limit the operation of subsection 187N(3), which item 31 inserts into the Bill.

Item 53 – Oversight of data journalist information warrants and authorisations

233. Item 53 will insert amending item 6X in Schedule 1 to the Bill. This item inserts proposed sections 185D and 185E in the TIA Act, to implement the Government's responses to PJCIS Report recommendations 27 and 34. Consequential on the introduction of journalist information warrants, the amendments require agencies' to provide a copy of journalist information warrants to the Minister, IGIS and Ombudsman.

Notification of relevant authorisations to oversight bodies and the Minister

234. Proposed section 185D will require the Director-General of Security and the Commissioner of the Australian Federal Police to provide copies of journalist information warrants to the IGIS or the Ombudsman (if applicable) as soon as practicable after they are made. The Commissioner of the Australian Federal Police is required to give the Minister a

copy of the warrant as soon as practicable and the Minister must then notify the PJCIS that such a warrant has been issued.

235. Furthermore, the proposed section will require the Director-General of Security and the chief officers of enforcement agencies to provide the IGIS or Ombudsman (as applicable) with copies of authorisations made under those warrants as soon as practicable after the expiry of the warrant.

236. Subsections 185D(1), (2), (5) and (6) will ensure that the relevant independent oversight bodies (the IGIS and Ombudsman) are provided with copies of journalist information warrants and authorisations made under those warrants. The IGIS and Ombudsman can then undertake relevant oversight activities in relation to the warrants and subsequent authorisations under their governing legislation – the IGIS Act, and in the case of the Ombudsman, the TIA Act.

Notification to the PJCIS of independent oversight outcomes for relevant authorisations

237. Proposed subsections 185D(3)-(4) and 185D(7)-(8) impose obligations on the Minister in relation to reports provided by the IGIS or Ombudsman concerning journalist information warrants and authorisations made as a result. In the event that the IGIS or the Ombudsman exercise their oversight functions in relation to relevant warrants and authorisations, and report to the responsible Minister in accordance with their governing legislation, the Minister is then required to provide copies of those oversight reports to the PJCIS as soon as practicable after receiving them from the IGIS or the Ombudsman.

238. The PJCIS can then request the IGIS or the Ombudsman to brief it on the relevant oversight report.

Reports on access to retained data

239. Proposed section 185E implements recommendation 34 of the PJCIS report. It imposes corresponding obligations to those in proposed section 185D on the Minister, after receiving oversight reports from the IGIS or the Ombudsman in relation to the purpose and manner of access to data by ASIO or the AFP generally.

240. The Minister must provide any oversight reports to the PJCIS as soon as practicable after receiving them from the IGIS or Ombudsman, and the PJCIS may request the IGIS or Ombudsman to brief it on the relevant oversight report.

241. These amendments will ensure that the PJCIS has visibility of the outcomes of independent oversight of authorisations undertaken by the IGIS and Ombudsman, under those bodies' governing legislation. Importantly, the amendments will also preserve the independent discretion of these oversight offices in setting their oversight priorities and performing their statutory functions. The amendments will further maintain the established

lines of reporting as between the IGIS and the Ombudsman and the relevant responsible Minister.

242. The ability of the PJCIS to request briefing on the outcomes of oversight in relation to the retained data activities of ASIO and the AFP (under Part 5.3 of the *Criminal Code*) is consistent with its existing ability to seek briefings from relevant entities, including the IGIS, under section 30 of the ISA.

Item 54 – Changes to reporting to the Minister

243. Item 54 will insert amending items 6Y and 6Z into the Bill, which amend section 186 of the TIA Act, which relates to the information required of agencies in reporting to the Minister. That information is included in the TIA Act Annual Report which is tabled in Parliament each year.

244. The report includes information about agency's use of powers under the TIA Act including information about interception warrants, warrants for access to stored communications and authorisations for access to telecommunications data. Amending items 6Y and 6Z expands the list of required information in accordance with recommendation 33 of the PJCIS Report, and will include the number of journalist information warrants issued during the reporting period and the number of authorisations made under those journalist information warrants.

245. Proposed subsection 186(1E) provides the Minister with a declaration-making power to declare additional kinds of information that must be provided under section 186(1).

Item 55 – Applications made before commencement of Part 5-1A

246. Item 55 amends the Bill by adding a reference to proposed subsection 187KA(2) to paragraph (1)(b) of item 9 in Part 3 of Schedule 1. Item 9 in Part 3 of Schedule 1 is an application provision governing applications made by service providers prior to the commencement of the legislation.

247. The effect of this amendment will be to provide that at any time after this legislation receives the Royal Assent, a service provider may apply to the ACMA for review of a decision by the CAC on an application by the service provider to exempt the service provider from some or all of its data retention obligations. However, the service provider will not be able to apply to ACMA unless and until the CAC has made such a decision.

248. The purpose of this amendment is to implement recommendation 15 of the PJCIS report in relation to the period after Royal Assent of the legislation, but prior to commencement of the legislation.

Item 56 – Decisions made before commencement of Part 5-1A

249. Item 56 amends the Bill by adding a reference to proposed section 187KA to clause (1) of item 10 in Part 3 of Schedule 1. Item 10 in Part 3 of Schedule 1 is an application provision governing the effect of decisions made prior to the commencement of the legislation. Proposed section 187KA provides for a power for ACMA to review a decision by the CAC in relation to an application by a service provider for exemption or variation of its data retention obligations.

250. The effect of this amendment will be to provide that, for the purposes of section 4 of the *Acts Interpretation Act 1901* (the AIA), the power to make a decision under section 187KA is taken to be a power to make an instrument of administrative character. Section 4 of the AIA allows for the exercise of powers of an administrative character conferred by an Act before commencement of that Act.

Item 57 – First reporting period after commencement of Part 5-1A

251. Item 57 amends the Bill by inserting a new provision into Part 3 of Schedule 1. This provision provides that, in the first annual reporting period following the commencement of the Bill, ASIO and enforcement agencies are only required to comply with the new annual reporting requirements introduced by the Bill on a prospective basis. That is, agencies will not be required to report on matters that occurred before commencement of the legislative requirements.

Schedule 2 Amendments

Item 58 – Listing of ASIC and ACCC

252. This item amends proposed subparagraph 110A(1)(e) by adding the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) to the list of agencies which are defined as a criminal law-enforcement agency.

253. The amendment implements recommendation 20 of the PJCIS Report by adding ASIC and ACCC as criminal law-enforcement agencies under proposed section 110A of the Bill. The effect of this amendment is to permit ASIC and ACCC to access stored communications (subject to a warrant), prospective data and, through status as an ‘enforcement agency’ (as part of the definition of a ‘criminal law-enforcement agency’) access to telecommunications data.

Item 59 – Declaration of criminal law-enforcement agencies

254. This item amends proposed paragraph 110A(3)(a) by replacing the reference to ‘the’ authority the Minister may declare to be a ‘criminal law-enforcement agency’ with a reference to ‘an’ authority the Minister may declare. This item corrects an error in drafting.

Item 60 – Declaration of criminal law-enforcement agencies

255. This item amends the Bill to insert a proposed subsection 110A(3A). Proposed subsection 110A(3A) clarifies that the Minister may declare an authority or body to be a criminal law-enforcement agency under subsection 110A(3), even if the head of that authority or body has not made a request in accordance with subsection 110A(2).

256. This item also amends the Bill to insert a proposed subsection 110A(3B). Proposed subsection 110A(3B) provides that the Minister may not declare an authority or body to be a criminal law-enforcement agency unless the Minister is satisfied on reasonable grounds that the authority or body has functions that include investigating serious contraventions. The term 'serious contravention' is defined in section 5E of the TIA Act.

257. Proposed subsection 110A(3B) implements recommendation 17 of the PJCIS Report. Proposed subsection 110A(3B) is intended to ensure that only agencies that investigate serious contraventions can be declared criminal law-enforcement agencies and thereby be able to use the more intrusive powers of obtaining stored communications warrants or making an authorisation for the disclosure of prospective telecommunications data.

Item 61 – Omission of paragraph 110A(4)(a)

258. Item 61 omits proposed paragraph 110A(4)(a) of the Bill, which required the Minister to 'have regard to' whether the functions of the authority or body included investigating serious contraventions when considering whether to declare an authority or body to be a criminal law-enforcement agency.

259. This item implements the relevant part of recommendation 17 of the PJCIS Report. Under proposed subsection 110A(3B), the Minister is required to be 'satisfied on reasonable grounds' that the functions of the authority or body include investigating serious contraventions. This new requirement supersedes the reference in proposed paragraph 110A(4)(a) of the Bill to the Minister being required to 'have regard to' this factor.

Item 62 – Omission of reference to 'those' serious contraventions

260. Item 62 amends the Bill by removing the reference to 'those' serious contraventions in paragraph 110A(4)(b). This item is consequential on the deletion of paragraph 110A(4)(a) effected by item 61. There is no further requirement to refer to 'those' serious contraventions.

Items 63, 64 and 65 – Privacy considerations with respect to 'criminal law-enforcement agency' declarations

261. Items 63, 64 and 65 will amend subparagraph 110A(4)(c)(ii) of the Bill to provide that the characteristics of a binding scheme in relation to the protection of personal information include a mechanism:

- for monitoring the authority or body's compliance with the scheme; and

- to enable individuals to seek recourse if their personal information is mishandled.

262. The effect of these items will require the Minister to be satisfied, in considering whether to make a declaration of an 'criminal law-enforcement agency', that the authority or body is required to comply with a binding scheme with the listed privacy-protection mechanisms. These items implement recommendation 18 of the PJCIS Report.

Item 66 – Declaration of criminal law-enforcement agency to expire after 40 sitting days

263. Item 66 amends the Bill to insert proposed subsections 110A(10) and 110A(11). The purpose of item 66 is to implement the relevant part of recommendation 17 of the PJCIS report, which was that declarations of criminal law-enforcement agencies should expire after 40 days and that any Bill to amend the TIA Act should be referred to the PJCIS for review.

264. Paragraph 110A(10)(a) provides that a declaration will come into force either when it is made or on a later day specified in the declaration. Paragraph 110A(10)(b) provides that the declaration ceases to be in force after 40 sitting days of either House of Parliament after the declaration comes into force. The time to expiry of the declaration will only commence once the declaration comes into force (which may be later than when it is made).

265. Subsection 110A(11) that when a Bill is introduced into either House of Parliament to amend the list of criminal law-enforcement agencies in the TIA Act, the Minister must refer the amending Bill to the PJCIS and give the PJCIS at least 15 sitting days of a House of Parliament to conduct its review and issue its report.

Item 67 – Declaration of enforcement agencies

266. This item amends proposed paragraph 176A(3)(a) (inserted as an amendment to item 4 in Part 1 of Schedule 2 of the Bill) by replacing the reference to 'the' authority the Minister may declare to be an 'enforcement agency' with a reference to 'an' authority the Minister may declare. This item corrects an error in drafting

Item 68 – Declaration of enforcement agencies

267. This item amends the Bill to insert a proposed subsection 176A(3A). Proposed subsection 176A(3A) clarifies that the Minister may declare an authority or body to be an enforcement agency under subsection 176A(3), even if the head of that authority or body has not made a request in accordance with subsection 176A(2).

268. This item also amends the Bill to insert a proposed subsection 176A(3B). Proposed subsection 176A(3B) provides that the Minister may not declare an authority or body to be an enforcement agency unless the Minister is satisfied on reasonable grounds that the authority or body has functions that include or more of:

- enforcement of the criminal law
- administering a law imposing a pecuniary penalty
- administering a law relating to the protection of the public revenue.

269. Proposed subsection 176A(3B) implements the relevant part of recommendation 21 of the PJCIS Report. Proposed subsection 176A(3B) is intended to ensure that only agencies that have the functions referred to above can be declared enforcement agencies and thereby be able to access historic telecommunications data.

Item 69 – Omission of paragraph 176A(4)(a)

270. Item 69 omits proposed paragraph 176A(4)(a) of the Bill, which required the Minister, when considering whether to declare an authority or body to be an enforcement agency, to 'have regard to' whether the authority or body has one or more of the following functions:

- enforcement of the criminal law
- administering a law imposing a pecuniary penalty
- administering a law relating to the protection of the public revenue.

271. This item implements the relevant part of recommendation 21 of the PJCIS Report, and is consequential on proposed subsection 176A(3B). Under proposed subsection 176A(3B), the Minister is required to be 'satisfied on reasonable grounds' that the functions of the authority or body include the functions referred to above. This new requirement supersedes the reference in proposed paragraph 176A(4)(a) of the Bill to the Minister being required to 'have regard to' this factor.

Item 70 – Omission of reference to 'those functions'

272. Item 70 amends the Bill by removing the reference to 'those functions' in paragraph 176A(4)(b). The reference to 'those functions' includes the enforcement of a criminal law, pecuniary penalty or protection of public revenue in proposed paragraph 176A(4)(a) of the Bill.

273. This item is consequential on the deletion of paragraph 176A(4)(a) effected by item 69 and the insertion of subsections 176A(3A) and (3B). There is no further reference to 'those functions' as this has been substituted by 'the functions referred to in subsection (3B)' which includes the enforcement of a criminal law, pecuniary penalty or protection of public revenue.

Items 71, 72 and 73 – Privacy considerations with respect to 'enforcement agency' declarations

274. Items 71, 72 and 73 will amend subparagraph 176A(4)(c)(ii) of the Bill to provide that the characteristics of a binding scheme in relation to the protection of personal information include a mechanism:

- for monitoring the authority or body's compliance with the scheme; and
- to enable individuals to seek recourse if their personal information is mishandled.

275. The effect of these items will require the Minister to be satisfied, in considering whether to make a declaration of an 'enforcement agency', that the authority or body is required to comply with a binding scheme with the privacy-protection mechanisms. These items implement recommendation 22 of the PJCIS Report.

Item 74 – Declaration of enforcement agency to expire after 40 sitting days

276. Item 74 amends the Bill to insert proposed subsections 176A(10) and (11). The purpose of item 74 is to implement the relevant part of recommendation 21 of the PJCIS report, which was that declarations of law enforcement agencies should expire after 40 days and that any Bill to amend the TIA Act be referred to the PJCIS for review.

277. Paragraph 176A(10)(a) provides that the declaration will come into force either when it is made or on a later day specified in the declaration. Paragraph 176A(10)(b) provides that the declaration ceases to be in force after 40 sitting days of either House of Parliament after the declaration comes into force. The time to expiry of the declaration will only commence once the declaration comes into force (which may be later than when it is made).

278. Subsection 176A(11)(a) provides that when a Bill is introduced into either House of Parliament to amend the list of enforcement agencies in the TIA Act the Minister must refer the amending Bill to the PJCIS and give the PJCIS at least 15 sitting days of a House of Parliament to conduct its review and issue its report.