THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

PRIVACY AMENDMENT (RE-IDENTIFICATION OFFENCE) BILL 2016

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, Senator the Hon George Brandis QC)
PRIVACY AMENDMENT (RE-IDENTIFICATION OFFENCE) BILL 2016

GENERAL OUTLINE

1. This Bill amends the Privacy Act 1988 (the Privacy Act) to introduce provisions which prohibit conduct related to the re-identification of de-identified personal information published or released by Commonwealth entities.

2. The publication of government datasets, including de-identified data, enables the government, policymakers, researchers, and other interested persons to take full advantage of the opportunities that new technology creates to improve research and policy outcomes. However, with advances in technology, methods that were sufficient to de-identify data in the past may become susceptible to re-identification in the future. The Bill is intended to act as a deterrent against attempts to re-identify de-identified personal information in government datasets and introduces criminal and civil penalties for the prohibited conduct.

3. The Bill introduces specific offences and civil penalty provisions which provide that:
   - de-identified personal information must not intentionally be re-identified, and
   - re-identified personal information must not intentionally be disclosed.

4. A further civil penalty provision provides that an entity must notify a responsible agency if the entity re-identifies de-identified personal information (intentionally or otherwise), and comply with any directions from the agency about the handling of the information.

5. Once an agency becomes aware that the information is no longer de-identified it may provide directions for dealing with the information and must inform the Australian Information Commissioner (the Commissioner). The Bill provides the Commissioner with powers to investigate the matter.

6. Under the Bill, de-identified personal information is information that has been published by, or on behalf of, an agency in a generally available publication on the basis that it was de-identified personal information. This will limit the application of the Bill to government datasets that are made generally available to the public.

7. Entities subject to the Bill include organisations, including small businesses, as well as individuals. The Bill has a wider scope than the general provisions of the Privacy Act, which does not generally apply to small businesses and individuals. This wider scope reflects the importance of a general deterrent to the re-identification of de-identified personal information, rather than a deterrent limited to entities subject to the Privacy Act.

8. The Bill does not apply to agencies, Commonwealth contracted service providers and entities that enter into agreements with agencies if re-identification:
   - was done in connection with the agency’s functions or activities or was required or authorised to be done by or under Australian law,
   - was done for the purposes of meeting (directly or indirectly) an obligation under a Commonwealth contract, or
was done for the purposes of an agreement with the agency.

9. These exclusions will ensure these entities are not captured by the Bill’s offences when engaging in ordinary functions and activities such as decryption activities to test information security. The Bill also provides that the Minister may exempt entities from the operation of the Bill if the Minister is satisfied there is a public interest to do so.

10. Entities that contravene the prohibitions contained in the Bill face a criminal offence punishable by imprisonment for 2 years or 120 penalty units or a civil penalty of up to 600 penalty units. These criminal offence and civil penalty provisions are intended to act as a strong deterrent against the re-identification of de-identified personal information. The offences apply retrospectively to conduct engaged in on or after 29 September 2016. This is intended to make conduct that occurred after the Government announcement it would introduce the Bill subject to the provisions of the Bill.

11. Similar measures to those in the Bill have been considered in the United Kingdom (the UK). The Review of Data Security, Consent and Opt-Outs by the UK’s National Data Guardian for Health and Care recommended the UK Government consider introducing stronger sanctions to protect anonymised data including criminal penalties for the re-identification of individuals.

Financial impact statement

12. This Bill has no significant impact on Commonwealth expenditure or revenue.
STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

Privacy Amendment (Re-identification Offence) Bill 2016

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

Overview of the Bill

14. The Privacy Amendment (Re-identification Offence) Bill 2016 (the Bill) amends the Privacy Act 1988 (Privacy Act) by introducing provisions to prohibit conduct related to the re-identification of de-identified personal information published by responsible agencies.

15. The Bill introduces specific offences which provide that:
   - de-identified personal information must not intentionally be re-identified (section 16D)
   - re-identified personal information must not intentionally be disclosed (section 16E), and
   - an entity must:
     - notify a responsible agency if de-identified personal information is re-identified, intentionally or unintentionally,
     - cease any other use or disclosure of the re-identified information, and
     - comply with any directions from the agency about the handling of the information (section 16F).

16. These offences would apply from 29 September 2016. This commencement date is intended to be a strong deterrent against attempts to re-identify de-identified personal information in government datasets while the Bill is considered by the Parliament.

17. An entity contravening section 16D or 16E faces a criminal penalty of 2 years imprisonment or 120 penalty units, or a civil penalty of 600 penalty units. No criminal penalty applies to contraventions of section 16F, though a civil penalty of 200 penalty units applies to contraventions of each of the three elements of the section.

18. The Bill includes a power for the Attorney-General to make a determination by legislative instrument which would exempt an entity from the offences for particular purposes, after the Attorney-General has consulted with the Australian Information Commissioner (the Commissioner).
Human rights implications

19. The Bill engages the following rights:
   - the right to privacy in article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)
   - the right to freedom of expression in article 19 of the ICCPR
   - the right to a fair trial in article 14 of the ICCPR, and
   - the prohibition on retrospective criminal laws in article 15 of the ICCPR

Right to privacy

20. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honour and reputation. Article 17 further provides that everyone has the right to the protection of the law against such interference or attacks.

21. In accepting the benefits of the release of de-identified datasets, the Government also recognises that the privacy of citizens is of paramount importance, and the importance of Government agencies effectively de-identifying information which is published, to minimise the possibility that individuals who are the subject of that data are reasonably identifiable.

22. The Bill promotes the right to privacy by making intentional re-identification of this de-identified data, and intentional disclosure of re-identified information unlawful, in accordance with article 17 of the ICCPR. The potential for imprisonment and financial penalties will have a deterrent effect on entities considering re-identification of de-identified information or disclosure of re-identified information.

23. The Bill also promotes the right to privacy by providing that, where an entity intentionally or unintentionally re-identifies this information, the entity must notify the responsible agency (who in turn must notify the Commissioner), cease any other use or disclosure of the information and comply with any orders from the agency about the handling of the information. This will ensure appropriate handling of re-identified information, even where that re-identification was unintentional. More broadly, this requirement will provide systemic privacy benefits for Australians by ensuring that agencies and the Commissioner become aware of instances where Government data has been re-identified, and steps can be taken to withdraw the relevant data from any further public access prior to adopting improved de-identification processes (where possible), and to consider whether any other datasets are vulnerable to equivalent vulnerabilities.

24. These measures in the Bill promote and protect the right to privacy.

Right to freedom of expression

25. Article 19 of the ICCPR provides that everyone shall have the right to freedom of expression. This right shall include 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 of his choice.
26. The exercise of the right to freedom of expression carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for respect of the rights or reputations of others, or for the protection of national security or of public order, or of public health or morals.

27. Unlike some other offences, breaches of privacy cannot be easily remedied because the publication of private information cannot be reversed. The Bill makes re-identification of de-identified information and associated conduct unlawful. These offences limit the right to freedom of expression by restricting the ability of individuals to receive and impart certain kinds of information. However, these offences are necessary to protect the rights and reputations of individuals, particularly their right to privacy.

28. These measures in the Bill are consistent with the right to freedom of expression.

Right to a fair trial

29. Article 14 of the ICCPR guarantees a person be afforded, in the determination of any criminal charge against them, the right to a fair trial. The United Nations Human Rights Committee has stated that the notion of criminal charges may ‘also extend to acts that are criminal in nature with sanctions that, regardless of their qualification in domestic law, must be regarded as penal because of their purpose, character or severity’ (see General Comment No. 32, paragraph 15; Communication No. 1015/2001, Perterer v Austria, at paragraph 9.2). It is therefore necessary to consider the substance as well as the form of both the criminal and civil penalties provided for by the Bill (excluding the prohibition on retrospective criminal offences in article 15 of the ICCPR, which is addressed separately below).

Level of criminal penalties and civil penalties

30. The criminal penalties in sections 16D and 16E and the civil penalties in sections 16D, 16E and 16F are set at an upper limit intended to appropriately respond to deliberate re-identification and disclosure of re-identified personal information that may be ‘sensitive information’, as defined in existing subsection 6(1) of the Privacy Act (for example, health information). It is intended that, for re-identification activities involving personal information that is not ‘sensitive information’, a court would have discretion to impose a lesser criminal or civil penalty reflecting the nature of the information involved and all the relevant circumstances.

31. In addition, no criminal penalties apply under section 16F and the civil penalty provision is set at a lower level than sections 16D and 16E. This reflects that section 16F also captures unintentional re-identification, which should not attract criminal penalties or civil penalties equivalent to those which apply under sections 16D and 16E. As with civil penalties under sections 16D and 16E, it is also intended that the upper limit of civil penalties under section 16F would apply only in particularly serious cases where the entity has failed to comply with section 16F (for example, if the entity is aware that it has unintentionally re-identified health information but then fails to notify the responsible agency that the information is vulnerable to re-identification).
32. The civil penalties in sections 16D, 16E and 16F are also deliberately set at a lower level than the existing civil penalty of 2000 penalty units that may apply for serious and repeated interference with the privacy of an individual under existing section 13G of the Privacy Act. This reflects that the civil penalties in sections 16D, 16E and 16F will target a broader range of entities and a more limited form of conduct than existing civil penalty provisions in the Privacy Act (although existing section 80W of the Privacy Act providing that a body corporate may be subject to a pecuniary penalty 5 times the amount of the penalty specified in a civil penalty provision of the Privacy Act will still apply to pecuniary penalties under sections 16D, 16E and 16F).

33. Relevantly, the Privacy Act’s civil penalty provisions, including the civil penalty provisions in sections 16D, 16E and 16F, also incorporate appropriate safeguards. These include the stipulation that in determining pecuniary penalties a court must take all relevant matters into account, including the circumstances of the contravention, the nature and extent of any loss or damage suffered because of the contravention and whether the entity has previously been found to have engaged in similar conduct.

34. For these reasons, the level of criminal penalties which apply under sections 16D and 16E and the level of civil penalties which apply under sections 16D, 16E and 16F are a reasonable and appropriate response to the behaviours the penalties are intended to discourage.

Application of both criminal and civil penalties in sections 16D and 16E

35. Sections 16D and 16E of the Bill contain both criminal and civil penalties for the same conduct. The intention of the provisions is that, where criminal penalties cannot or will not be imposed on an entity who contravenes the provisions, the Commissioner may investigate and may decide to apply to the Federal Court or Federal Circuit Court to impose a civil penalty.

36. The Bill contains protections and engages existing protections under the Privacy Act to ensure that entities will not be subject to both criminal and civil penalties for the same conduct. For example, under existing section 80ZD of the Privacy Act an entity cannot be subject to a civil penalty under the Privacy Act if they have been convicted of an offence relating to conduct that is the same, or substantially the same, as the conduct that contravened the civil penalty provision. In addition, existing section 80ZE of the Privacy Act provides that any proceedings for a civil penalty provision under the Act are automatically stayed if criminal proceedings are commenced or have already commenced against the entity for an offence involving conduct that is the same, or substantially the same, as the conduct that contravened the civil penalty provision.

37. Items 14, 15, 16 and 17 amend existing section 49 of the Privacy Act to ensure that, if the Commissioner refers a possible contravention of an offence under section 16D or 16E to the Commissioner of Police or Director of Public Prosecutions, any investigation by the Commissioner into whether the conduct was also a possible contravention of the civil penalty provision must cease until the Commissioner of Police or Director of Public Prosecutions advises the Commissioner that the matter will not be, or will no longer be, subject to proceedings for a criminal offence.
38. These provisions together ensure that the imposition of both criminal and civil penalties for the same conduct will not result in entities being punished twice for the same conduct.

Reverse burden offences

39. Defences in sections 16D, 16E and 16F require entities to demonstrate that their behaviour was consistent with the relevant defences in each section, specifically that:

- the entity was a contracted service provider for a Commonwealth contract to provide services for a responsible agency, and the act was done for the purpose of meeting (directly or indirectly) an obligation under the contract,

- the entity has entered into an agreement with the responsible agency to perform functions or activities on behalf of the agency, and the act was done in accordance with the agreement, or

- the entity is an exempt entity for the purpose of a determination in force under section 16G, and the act was done for a purpose specified in the determination and in compliance with any conditions specified in the determination.

40. This is contrary to the general situation where consistency with the presumption of innocence under article 14(2) of the ICCPR requires the prosecution to prove each element of a criminal offence beyond reasonable doubt.

41. However, for each of the three defences it is expected that each limb of the defence will not be unreasonably difficult for an entity to prove. That is, it is expected that it will not be unreasonably difficult for an entity to demonstrate that it is a contracted service provider for a Commonwealth contract to a responsible agency, has entered into an agreement to perform functions or activities on behalf of a responsible agency, or is an exempt entity for the purpose of a determination in force under section 16G. It follows that, given a Commonwealth contract, agreement to perform functions or activities on behalf of an agency or a determination under section 16G would all be expected to be focused on achieving specific outcomes, it should not be unreasonably difficult for an entity to prove that the act falling under the defence was done for purposes of achieving those outcomes. This also reflects the seriousness of the conduct that is otherwise prohibited under section 16D, 16E or 16F, where the above defences do not apply.

42. Given the nature of these defences, it is expected that prosecutions will not proceed where it is clear to authorities that the entity will be able to rely on an applicable defence during the proceedings.

43. For these reasons the reverse burden offences contained in the Bill are a reasonable and appropriate response to the behaviours the penalties are intended to discourage.
Prohibition on retrospective criminal laws

44. Article 15 of the ICCPR provides that no one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence at the time when it was committed.

45. Retrospective offences challenge a key element of the rule of law — that laws are capable of being known in advance so that people subject to those laws can exercise choice and order their affairs accordingly.

46. The Bill provides that new offences relating to the re-identification of de-identified information operate from 29 September 2016. The Government does not propose to make these offences lightly.

47. The retrospective application of the offences is reasonable and necessary. The Government has made it abundantly clear that it is pursuing this course of action. The Attorney-General’s media release (‘Amendment to the Privacy Act to further protect de-identified data’, 28 September 2016) states unequivocally that the offences will take effect from the date of announcement. Re-identification of de-identified information and associated conduct undertaken before the announcement is not prohibited by the Bill.

48. This action is necessary because releases of private information can have significant consequences for individuals beyond their privacy and reputation, which cannot be easily remedied. This warrants swift and decisive action by the Government to prohibit such conduct. Further, the retrospective commencement of the offences creates a strong disincentive for entities to engage in such conduct while the Parliament considers the Bill.

49. The retrospective application of the offences is proportionate as it is for a short time period, and steps have been taken to ensure it is no more retrospective than required. The Government has introduced this Bill in the Parliament at the earliest available opportunity.

50. These measures in the Bill are consistent with the prohibition on retrospective criminal laws.

Conclusion

51. The Bill is compatible with human rights because it promotes the protection of human rights, particularly the right to privacy in article 17 of the ICCPR. To the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate to achieve the legitimate aims of the Bill and the Privacy Act.
NOTES ON CLAUSES

Preliminary

Clause 1—Short title

1. This clause provides for the short title of the Act to be the *Privacy Amendment (Re-identification Offence) Act 2016*.

Clause 2—Commencement

2. This clause provides for the commencement of each provision in the Bill as set out in the table.

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

4. Item 2 in the table provides that Schedule 1 of the Bill, which contains the substantive amendments to the *Privacy Act 1988* (*the Privacy Act*), will commence on the day after the Act receives the Royal Assent.

5. Subclause 2(2) provides that the information in column 3 of the table, which provides dates and further details, does not form part of the Bill. The subclause also provides that information in column 3 may be edited or inserted in any published version of the Bill once enacted.

Clause 3—Schedules

6. Clause 3 provides that each Act specified in the Schedule is amended or repealed as set out in the Schedule. Clause 3 also provides that any other item in a Schedule of the Bill will have effect according to its terms.

Schedule 1—Amendments

Part 1—Main amendments

*Privacy Act 1988*

Item 1 Subsection 7B(1) (note)

7. This item replaces ‘Note’ with ‘Note 1’, which will enable a ‘Note 2’ to be added to subsection 7B(1) by Item 2 of Schedule 1.
**Item 2** At the end of subsection 7B(1)

8. This item adds a ‘Note 2’ to the end of subsection 7B(1), which notes the subsection is affected by subsection 16CA(1) of the Bill. The effect of subsection 16CA(1) of the Bill on subsection 7B(1) is outlined in Item 5 below.

**Item 3** Subsection 7B(2) (note)

9. This item replaces ‘Note’ with ‘Note 1’, which will enable a ‘Note 2’ to be added to subsection 7B(2) by Item 4 of Schedule 1.

**Item 4** At the end of subsection 7B(2)

10. This item adds a ‘Note 2’ to the end of subsection 7B(2), which notes the subsection is affected by subsection 16CA(1) of the Bill. The effect of subsection 16CA(1) of the Bill on subsection 7B(2) is outlined in Item 5 below.

**Item 5** After Division 2 of Part III

**Division 3—Re-identification of de-identified personal information**

11. This item inserts a new Division 3 of Part III titled ‘Re-identification of de-identified personal information’ after the existing Division 2. This new Division contains the substantive elements of the re-identification offence provisions.

12. The Division is divided into five sections. Broadly, the first section provides for the application of Division 3 in relation to certain acts, the second section creates an offence which provides that de-identified personal information must not be re-identified, the third section creates an offence which provides that re-identified personal information must not be disclosed, the fourth section creates a requirement which provides that an entity must notify a responsible agency if de-identified personal information is re-identified, and the fifth section provides the Minister may determine that an entity is an exempt entity for certain purposes.

**Section 16CA Application of this Division in relation to certain acts**

13. Section 16CA provides for the application of Division 3 in relation to certain acts. Subsection 16CA(1) provides that certain acts are not exempt for the purposes of paragraph 7(1)(ee) of the Privacy Act.

14. Paragraph 16CA(1)(a) provides that an act done by an organisation that is an individual is not, despite subsection 7B(1) of the Privacy Act, exempt for the purposes of paragraph 7(1)(ee) of the Privacy Act if the act is a contravention of subsection 16D(1) or 16E(1) or 16F(3), (4) or (10) of the Bill.

15. Paragraph 16CA(1)(a) brings the non-business related acts of individuals, generally excluded from the scope of the Privacy Act through the combined effect of subsection 7B(1) and paragraph 7(1)(ee) of the Privacy Act, within the scope of the Bill relating to the re-identification of de-identified personal information. The Bill makes the non-business
related acts of individuals subject to the Bill’s provisions due to the need for a general deterrent to the re-identification of de-identified personal information, rather than a deterrent limited to entities subject to the Privacy Act, which would otherwise exclude the non-business related acts of individuals.

16. Paragraph 16CA(1)(b) provides that an act done by an organisation referred to in paragraphs 7B(2)(a) and (b) of the Privacy Act is not, despite subsection 7B(2) of the Privacy Act, exempt for the purposes of paragraph 7(1)(ee) of the Privacy Act if the act is a contravention of subsection 16D(1) or 16E(1) or 16F(3), (4) or (10) of the Bill.

17. An organisation referred to in paragraphs 7B(2)(a) and (b) of the Privacy Act is an organisation that is a contracted service provider for a Commonwealth contract that would be a small business operator (i.e. have an annual turnover of $3 million or less) if it were not a contracted service provider for a Commonwealth contract, and would therefore normally be exempt from the Privacy Act in relation to all acts not done for the purpose of meeting (directly or indirectly) an obligation under the Commonwealth contract. The effect of paragraph 16CA(1)(b) of the Bill is to bring the acts of such an organisation, generally excluded from the scope of the Privacy Act by the combined effect of subsection 7B(2) and paragraph 7(1)(ee) of the Privacy Act, within the scope of the Bill. The Bill makes the acts of organisations referred to in paragraphs 7B(2)(a) and (b) of the Privacy Act subject to the Bill due to the need for a general deterrent to the re-identification of de-identified personal information, rather than a deterrent limited to entities subject to the Privacy Act, which would otherwise exclude such organisations. In addition, the exclusion from the scope of the Bill of a subset of small businesses operators would be inconsistent with the inclusion of small businesses operators within the scope of the Bill generally.

18. Subsection 16CA(2) is included to avoid doubt that the Division applies in relation to an act done by an entity that is employed by, or engaged to provide services to, a State or Territory authority, if the act is done other than in the performance of the entity’s duties of employment or in accordance with the entity’s contract for services. Subsection 16CA(2) clarifies that the activities of such entities done in the course of their official role with a State or Territory authority are captured by the general exemption of State and Territory authorities from the operation of the Privacy Act.

Section 16D De-identified personal information must not be re-identified

19. This section provides that de-identified personal information must not be re-identified.

20. Subsection 16D(1) provides that an entity contravenes the subsection if it re-identifies de-identified personal information if:

- information has been published by, or on behalf of, an agency (the responsible agency) in a generally available publication (paragraph 16D(1)(a)); and

- the information was published on the basis that it was de-identified personal information (paragraph 16D(1)(b)); and
on or after 29 September 2016, the entity does an act with the intention of achieving the result that the information is no longer de-identified (paragraph 16D(1)(c); and

- the act has the result that the information is no longer de-identified.

21. An entity is defined by subsection 6(1) of the Privacy Act to include an agency, organisation or small business operator. This means that small business operators are subject to section 16D. Small business operators are generally excluded from the operation of the Privacy Act through the combined operation of subsection 6C(1), and sections 6D and 6DA of the Privacy Act. Small businesses operators are included in the scope of section 16D, including the criminal offence and civil penalty provisions of subsection 16D(6) and (7), due to the need for a general deterrent to the re-identification of de-identified personal information, rather than a deterrent limited to entities subject to the Privacy Act, which would otherwise generally exclude small business operators.

22. Paragraph 16D(1)(a) means that de-identified personal information must be contained in a generally available publication rather than disclosed in other more limited circumstances by the responsible agency. The term ‘generally available publication’ is defined in subsection 6(1) of the Privacy Act to mean a publication that is, or will be, generally available to the public, whether or not it is published in print, electronically, or in any other form, and whether or not it is available on the payment of a fee.

23. Circumstances of disclosure that would not fall under subsection 16D(1) could include, for example, discrete disclosure by the responsible agency to a service provider for the provision of a service or to a researcher or research institution for research purposes. The provision in paragraph 16D(1)(a) that the information may also be published on behalf of an agency anticipates that if the responsible agency uses another party to publish the information in a generally available publication, then the re-identification by an entity of this information should also contravene subsection 16D(1).

24. The reference to information that ‘was published on the basis it was de-identified personal information’ in subsection 16D(1)(b) is intended to convey that the section applies where an agency intended the published information to be de-identified information, regardless of whether it was possible to re-identify the information. ‘De-identified’ is defined in subsection 6(1) of the Privacy Act to mean that information is not ‘de-identified’ where it is no longer about an identifiable or reasonably identifiable individual. This definition accords with the definition of ‘personal information’ in subsection 6(1), which (in short) is information about ‘an identifiable or reasonably identifiable individual’.

25. Though an agency which publishes inadequately de-identified personal information will not breach any provision of the Bill, the agency would nonetheless risk breaching existing provisions of the Australian Privacy Principles (APPs) in the Privacy Act which regulate handling, disclosure and access to personal information. The Bill also provides the Australian Information Commissioner (the Commissioner) with additional assessment powers to ensure appropriate independent oversight applies to agency de-identification activities (see Item 6 below).
26. Paragraph 16D(1)(c) provides that an entity must have the intention of achieving the de-identification of the information. As a result, an act done without this intention would not contravene subsection 16D(1) or be subject to the criminal offence and civil penalty provisions under subsection 16D(6) and (7) of the Bill. Section 16F provides for the unintentional re-identification of de-identified personal information.

27. Paragraph 16D(1)(c) applies retrospectively to an act done with the intention of achieving the result that the information is no longer de-identified on or after 29 September 2016 when the Government announced the introduction of the Bill and stated that offences will take effect from the date of announcement. This retrospectivity is necessary because releases of private information can have significant consequences for individuals beyond their privacy and reputation, which cannot be easily remedied. In addition, the retrospective commencement of the offences creates a strong disincentive for entities to engage in such conduct while the Parliament considers the Bill.

28. Contravention of subsection 16D(1) will be subject to the criminal offence and civil penalty provisions under subsections 16D(6) and (7) of the Bill.

29. Note 1 for subsection 16D(1) notes the ancillary offence provisions in Part 2.4 of the Criminal Code apply in relation to the offence created by subsection 16D(6) of the Bill. Specifically, section 11.1 (attempt), section 11.2 (aiding, abetting, counselling or procuring), section 11.4 (incitement) and section 11.5 (conspiracy).

30. Note 2 for subsection 16D(1) notes that section 80V of the Privacy Act, which deals with ancillary contravention of a civil penalty provision, applies in relation to subsection 16D(7) of the Bill. These ancillary contraventions include aiding, abetting, counselling, or procuring the contravention of the civil penalty provision.

31. The offence under section 16D(1), coupled with the effect of sections 16E and 16F below and availability of ancillary offences provisions under the Criminal Code and ancillary contravention provisions under the Privacy Act, is also intended to discourage a range of behaviours which might flow from the intentional re-identification of de-identified information. For example:

- If an entity intentionally re-identified de-identified information, then made available methods of doing so to others, the entity would likely have breached both section 16D(1) and ancillary provisions involving aiding and abetting others to commit the offence.
  - The entity may also have breached section 16F unless the entity had notified the responsible agency and ceased any further use or disclosure of the information (other than disclosure to the responsible agency). Notification under section 16F in turn would allow an agency to give the entity directions about the handling of the information, which would be expected to include destroying the re-identified information in most circumstances.

- If an entity made available the methods of re-identifying de-identified information to another entity, even where the first entity had not re-identified the information itself, the
entity might trigger ancillary provisions on grounds of aiding or abetting re-identification of de-identified information.

32. However, in either of the above examples, or in other similar scenarios, it is expected that the determinations power in section 16G will ensure that an appropriate range of research activities can still be undertaken to test or otherwise assess the effectiveness of de-identification techniques, and advise agencies of any shortcomings in those techniques, without engaging the offence provisions. Existing exemptions and exclusions in the Privacy Act (such as the exclusion of State or Territory Government entities, or the exemption for media organisations acting in the course of journalism) would also apply.

33. Subsection 16D(2) provides that subsection 16D(1) does not apply if the entity is an agency and the act was done in connection with the performance of the agency’s functions or activities; or was required or authorised to be done by or under an Australian law or a court/tribunal order. Subsection 16D(2) should be read alongside existing subsection 4(2) of the Privacy Act, which provides that nothing in the Privacy Act can render the Commonwealth liable for prosecution for an offence. The practical additional effect of subsection 16D(2), therefore, is that an agency cannot be subject to a civil penalty due to breaching subsection 16D(1) if the agency’s act falls within scope of subsection 16D(2).

34. The exemption of agencies from contravention of subsection 16D(1) and therefore from the criminal offence and civil penalty provisions under subsection 16D(6) and (7) of the Bill is justified as it will ensure agencies do not contravene subsection 16D(1) when engaging in their ordinary functions and activities such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

35. The note for subsection 16D(2) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16D(2). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, agencies are best placed to demonstrate that the act was done in connection with the performance of the agency’s functions or activities; or was required or authorised to be done by or under an Australian law or a court/tribunal order. It is expected that this will not be unreasonably difficult for an agency to prove.

36. Subsection 16D(3) provides that subsection 16D(1) does not apply if the entity is a contracted service provider for a Commonwealth contract to provide services to the responsible agency and the act was done for the purposes of meeting (directly or indirectly) an obligation under the contract. The exemption of such entities from contravention of subsection 16D(1) and therefore from the criminal offence and civil penalty provisions under subsection 16D(6) and (7) of the Bill is justified as it will ensure these entities do not contravene subsection 16D(1) when engaging in functions and activities for which they are contracted such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

37. The note for subsection 16D(3) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16D(3). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, these entities are best placed to demonstrate
that the act was done in connection with the performance of the agency’s functions or activities. It is expected that this will not be unreasonably difficult for an entity to prove.

38. Subsection 16D(4) provides that subsection 16D(1) does not apply if the entity has entered into an agreement with the responsible agency to perform functions or activities on behalf of the agency and the act was done in accordance with the agreement. Subsection 16D(3) is intended to apply in situations where an agency and an entity have a formal relationship of some kind that falls short of a contractual relationship of the kind that would be covered under subsection 16D(3) above. The exemption of such entities from contravention of subsection 16D(1) and therefore from the criminal offence and civil penalty provisions under subsection 16D(6) and (7) of the Bill is justified as it will ensure these entities do not contravene subsection 16D(1) when engaging in functions and activities which they have entered an agreement for such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

39. The note for subsection 16D(4) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16D(4). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, these entities are best placed to demonstrate that the act was done in connection with the performance of the agency’s functions or activities. It is expected that this will not be unreasonably difficult for an entity to prove.

40. Subsection 16D(5) provides that subsection 16D(1) does not apply if the entity is an exempt entity for the purposes of section 16D in accordance with a determination in force under section 16G of the Bill; and the act was done for a purpose specified in that determination in relation to the entity and in compliance with any condition specified in the determination. Section 16G of the Bill provides that the Minister may make an entity exempt from section 16D if the Minister is satisfied it is in the public interest to do so.

41. The note for subsection 16D(5) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16D(5). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, entities are best placed to demonstrate that they are an exempt entity due to a determination under section 16G of the Bill and the act was done for a purpose specified in that determination in relation to the entity. It is expected that this will not be unreasonably difficult for an entity to prove.

42. Subsection 16D(6) provides that an entity commits an offence if the entity contravenes subsection 16D(1). The penalty for this offence is imprisonment for two years or 120 penalty units. The penalty is set at an upper limit intended to appropriately respond to deliberate re-identification and disclosure of re-identified personal information that may be ‘sensitive information’, as defined in existing subsection 6(1) of the Privacy Act (for example, health information). It is intended that, for re-identification activities involving personal information that is not ‘sensitive information’, a court would have discretion to impose a lesser criminal penalty reflecting the nature of the information involved and all the relevant circumstances of the act.
43. Due to the retrospective application of paragraph 16D(1)(c), the criminal offence in subsection 16D(6) will apply retrospectively to a contravention of subsection 16D(1) that occurred on or after 29 September 2016. This retrospectivity is necessary because releases of private information can have significant consequences for individuals beyond their privacy and reputation, which cannot be easily remedied. In addition, the retrospective commencement of the offences creates a strong disincentive for entities to engage in such conduct while the Parliament considers the Bill.

44. Subsection 16D(7) provides that an entity is liable to a civil penalty of 600 penalty units if the entity contravenes subsection 16D(1). The penalty is set at an upper limit intended to appropriately respond to deliberate re-identification and disclosure of re-identified personal information that may be ‘sensitive information’, as defined in existing subsection 6(1) of the Privacy Act (for example, health information). It is intended that, for re-identification activities involving personal information that is not ‘sensitive information’, a court would have discretion to impose a lesser civil penalty reflecting the nature of the information involved and all the relevant circumstances of the act.

45. Subsections 16D(6) and (7) contain both criminal and civil penalties for the same conduct. The intention of the provisions is to ensure that, where criminal penalties cannot or will not be imposed on an entity who contravenes the provisions, the Australian Information Commissioner (the Commissioner) may investigate and may decide to apply to the Federal Court or Federal Circuit Court to impose a civil penalty.

46. Notably however, the Bill contains protections and engages existing protections under the Privacy Act to ensure that entities will not be subject to both criminal and civil penalties for the same conduct. For example, under existing section 80ZD of the Privacy Act an entity cannot be subject to a civil penalty under the Privacy Act if they have been convicted of an offence relating to conduct that is the same, or substantially the same, as the conduct that contravened the civil penalty provision. In addition, existing section 80ZE of the Privacy Act provides that any proceedings for a civil penalty provision under the Act are automatically stayed if criminal proceedings are commenced or have already commenced against the entity for an offence involving conduct that is the same, or substantially the same, as the conduct that contravened the civil penalty provision. Finally, items 14, 15, 16 and 17 amend existing section 49 of the Privacy Act, to ensure that, if the Commissioner refers a possible contravention of subsection 16D(1) to the Commissioner of Police or Director of Public Prosecutions, any investigation by the Commissioner into whether the conduct was also a possible contravention of the civil penalty provision must cease until such point (if any) where the Commissioner of Police or Director of Public Prosecutions advises the Commissioner that the matter will not be, or will no longer be, subject to proceedings for a criminal offence. These provisions together ensure that the imposition of both criminal and civil penalties for the same conduct will not result in entities being punished twice for the same conduct.

Section 16E Re-identified personal information must not be disclosed

47. This section provides that re-identified personal information must not be disclosed.

48. Subsection 16E(1) provides that an entity contravenes the subsection if:
• information has been published by, or on behalf of, an agency (the responsible agency) in a generally available publication (paragraph 16E(1)(a)); and

• the information was published on the basis that it was de-identified personal information (paragraph 16E(1)(b)); and

• on or after 29 September 2016, the entity does an act that has the result that the information is no longer de identified (paragraph 16E(1)(c)); and

• the entity is aware that the information is no longer de-identified (paragraph 16E(1)(d)); and

• on or after 29 September 2016 the entity discloses the information to a person or entity other than the responsible agency (paragraph 16E(1)(e)).

49. An entity is defined by subsection 6(1) of the Privacy Act to include an agency, organisation or small business operator. This means that small business operators are subject to section 16E. Small business operators are generally excluded from the operation of the Privacy Act through the combined operation of subsection 6C(1), and sections 6D and 6DA of the Privacy Act. Small businesses operators are included in the scope of section 16D, including the criminal offence and civil penalty provisions of subsection 16E(7) and (8), due to the need for a general deterrent to the re-identification of de identified personal information, rather than a deterrent limited to entities subject to the Privacy Act, which would otherwise generally exclude small business operators.

50. Paragraph 16E(1)(a) means that de-identified personal information must be contained in a generally available publication rather than disclosed in other more limited circumstances by the responsible agency. The term ‘generally available publication’ is defined in subsection 6(1) of the Privacy Act to mean a publication that is, or will be, generally available to the public, whether or not it is published in print, electronically, or in any other form, and whether or not it is available on the payment of a fee.

51. Circumstances of disclosure that would not fall under subsection 16E(1) could include, for example, disclosure under agreement by the responsible agency to a service provider for the provision of a service or to a researcher or research institution for research purposes. The provision in paragraph 16E(1)(a) that the information may also be published on behalf of an agency anticipates that if the responsible agency uses another party to publish the information in a generally available publication, then the re-identification by an entity of this information should also contravene subsection 16E(1).

52. The reference to information that ‘was published on the basis it as de-identified personal information’ in subsection 16E(1)(b) is intended to convey that the section applies where an agency intended the published information to be de-identified information, regardless of whether it was possible to re-identify the information. ‘De-identified’ is defined in subsection 6(1) of the Privacy Act to mean that information is not ‘de-identified’ where it is no longer about an identifiable or reasonably identifiable individual. This definition
accords with the definition of ‘personal information’ in subsection 6(1), which (in short) is information about ‘an identifiable or reasonably identifiable individual’.

53. Though an agency which publishes inadequately de-identified personal information will not breach any provision of the Bill, the agency would nonetheless risk breaching existing provisions of the APPs in the Privacy Act which regulate handling, disclosure and access to personal information. The Bill also provides the Commissioner with additional assessment powers to ensure appropriate independent oversight applies to agency de-identification activities (see Item 6 below).

54. Paragraph 16E(1)(c) provides that an entity must have done an act that has the result of achieving the de-identification of the information. As a result, information that is de-identified intentionally and unintentionally is subject to paragraph 16E(1)(c) as provided for in subsection 16E(2) of the Bill.

55. Paragraph 16E(1)(c) applies retrospectively to an act by an agency on or after 29 September 2016 that has the result that the information is no longer de-identified on or after 29 September 2016 when the Government announced the introduction of the Bill.

52. Paragraph 16E(1)(d) provides that an entity must be aware that the information is no longer de-identified. This will mean that if the entity is not aware the information it discloses is no longer de-identified the disclosure will not contravene subsection 16E(1).

56. Paragraph 16E(1)(e) applies retrospectively to the disclosure of information by an entity to a person or entity other than the responsible agency on or after 29 September 2016 when the Government announced the introduction of the Bill and stated that offences will take effect from the date of announcement. This retrospectivity is necessary because releases of private information can have significant consequences for individuals beyond their privacy and reputation, which cannot be easily remedied. In addition, the retrospective commencement of the offences creates a strong disincentive for entities to engage in such conduct while the Parliament considers the Bill.

53. Paragraph 16E(1)(e) provides that disclosure of the information to the responsible agency would not contravene subsection 16E(1). This anticipates section 16F of the Bill, which requires an entity to notify the responsible agency if de-identified personal information is re-identified.

54. Note 1 for subsection 16E(1) notes the ancillary offence provisions in Part 2.4 of the Criminal Code apply in relation to the offence created by subsection 16E(7) of the Bill. Specifically, section 11.1 (attempt), section 11.2 (aiding, abetting, counselling or procuring), section 11.4 (incitement) and section 11.5 (conspiracy).

55. Note 2 for subsection 16E(1) notes that section 80V of the Privacy Act, which deals with ancillary contravention of a civil penalty provision, applies in relation to subsection 16E(8) of the Bill. These ancillary contraventions include aiding, abetting, counselling, or procuring the contravention of the civil penalty provision.
56. Subsection 16E(2) provides that paragraph 16E(1)(c) applies regardless of whether the entity intended the act to have the result that the information is no longer de-identified. This means that the entity may contravene subsection 16E(1) regardless of whether the information was de-identified intentionally or unintentionally by the entity (though the entity would also need to be aware that the information was no longer de-identified to contravene subsection 16E(1), as per paragraph 16E(1)(d) above).

57. Subsection 16E(3) provides that subsection 16E(1) does not apply if the entity is an agency and the act was done in connection with the performance of the agency’s functions or activities; or was required or authorised to be done by or under an Australian law or a court/tribunal order. Subsection 16E(2) should be read alongside existing subsection 4(2) of the Privacy Act, which provides that nothing in the Privacy Act can render the Commonwealth liable for prosecution for an offence. The practical additional effect of subsection 16E(2), therefore, is that an agency cannot be subject to a civil penalty due to breaching subsection 16E(1) if the agency’s act falls within scope of subsection 16E(2).

58. The exemption of agencies from contravention of subsection 16E(1) and therefore from the criminal offence and civil penalty provisions under subsection 16E(7) and (8) of the Bill is justified as it will ensure agencies do not contravene subsection 16E(1) when engaging in their ordinary functions and activities such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

59. The note for subsection 16E(3) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16E(3). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, agencies are best placed to demonstrate that the act was done in connection with the performance of the agency’s functions or activities; or was required or authorised to be done by or under an Australian law or a court/tribunal order. It is expected that this will not be unreasonably difficult for an entity to prove.

60. Subsection 16E(4) provides that subsection 16E(1) does not apply if the entity is a contracted service provider for a Commonwealth contract to provide services to the responsible agency and the act was done for the purposes of meeting (directly or indirectly) an obligation under the contract. The exemption of such entities from contravention of subsection 16E(1) and therefore from the criminal offence and civil penalty provisions under subsection 16E(7) and (8) of the Bill is justified as it will ensure these entities do not contravene subsection 16E(1) when engaging in functions and activities for which they are contracted such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

61. The note for subsection 16E(4) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16E(4). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, these entities are best placed to demonstrate that the act was done in connection with the performance of the agency’s functions or activities. It is expected that this will not be unreasonably difficult for an entity to prove.
Subsection 16E(5) provides that subsection 16E(1) does not apply if the entity has entered into an agreement with the responsible agency to perform functions or activities on behalf of the agency and the act was done in accordance with the agreement. Subsection 16E(5) is intended to apply in situations where an agency and an entity have a formal relationship of some kind that falls short of a contractual relationship of the kind that would be covered under subsection 16E(4) above. The exemption of such entities from contravention of subsection 16E(1) and therefore from the criminal offence and civil penalty provisions under subsection 16E(7) and (8) of the Bill is justified as it will ensure these entities do not contravene subsection 16E(1) when engaging in functions and activities which they have entered an agreement for such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

The note for subsection 16E(5) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16E(5). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, these entities are best placed to demonstrate that the act was done in connection with the performance of the agency’s functions or activities. It is expected that this will not be unreasonably difficult for an entity to prove.

Subsection 16E(6) provides that subsection 16E(1) does not apply if the entity is an exempt entity for the purposes of section 16E in accordance with a determination in force under section 16G of the Bill; and the act was done for a purpose specified in that determination in relation to the entity and in compliance with any condition specified in the determination. Section 16G of the Bill provides that the Minister may make an entity exempt from section 16E if the Minister is satisfied it is in the public interest to do so.

The note for subsection 16E(6) notes that in criminal proceedings, a defendant bears an evidential burden in relation to the matter in subsection 16E(6). This is the reverse of the principle in criminal law that the prosecution must prove every element of the offence. This is justified by the fact that, in the circumstances, entities are best placed to demonstrate that they are an exempt entity due to a determination under section 16G of the Bill and the act was done for a purpose specified in that determination in relation to the entity. It is expected that this will not be unreasonably difficult for an entity to prove.

Subsection 16E(7) provides that an entity commits an offence if the entity contravenes subsection 16E(1) the penalty for which is imprisonment for two years or 120 penalty units. The penalty is set at an upper limit intended to appropriately respond to deliberate re-identification and disclosure of re-identified personal information that may be ‘sensitive information’, as defined in existing subsection 6(1) of the Privacy Act (for example, health information). It is intended that, for re-identification activities involving personal information that is not ‘sensitive information’, a court would have discretion to impose a lesser criminal penalty reflecting the nature of the information involved and all the relevant circumstances of the act.

Due to the retrospective application of paragraphs 16E(1)(c) and (e) the criminal offence in subsection 16E(7) will apply retrospectively to a contravention of subsection 16E(1) that occurred on or after 29 September 2016. This retrospectivity is
necessary because releases of private information can have significant consequences for individuals beyond their privacy and reputation, which cannot be easily remedied. In addition, the retrospective commencement of the offences creates a strong disincentive for entities to engage in such conduct while the Parliament considers the Bill.

68. Subsection 16E(8) provides that an entity is liable to a civil penalty of 600 penalty units if the entity contravenes subsection 16E(1). The penalty is set at an upper limit intended to appropriately respond to deliberate re-identification and disclosure of re-identified personal information that may be ‘sensitive information’, as defined in existing subsection 6(1) of the Privacy Act (for example, health information). It is intended that, for re-identification activities involving personal information that is not ‘sensitive information’, a court would have discretion to impose a lesser civil penalty reflecting the nature of the information involved and all the relevant circumstances of the act.

69. Subsections 16E(7) and (8) contain both criminal and civil penalties for the same conduct. The intention of the provisions is to ensure that, where criminal penalties cannot or will not be imposed on an entity who contravenes the provisions, the Commissioner may investigate and may decide to apply to the Federal Court or Federal Circuit Court to impose a civil penalty.

70. Notably however, the Bill contains protections and engages existing protections under the Privacy Act to ensure that entities will not be subject to both criminal and civil penalties for the same conduct. For example, under existing section 80ZD of the Privacy Act an entity cannot be subject to a civil penalty under the Privacy Act if they have been convicted of an offence relating to conduct that is the same, or substantially the same, as the conduct that contravened the civil penalty provision. In addition, existing section 80ZE of the Privacy Act provides that any proceedings for a civil penalty provision under the Act are automatically stayed if criminal proceedings are commenced or have already commenced against the entity for an offence involving conduct that is the same, or substantially the same, as the conduct that contravened the civil penalty provision. Finally, Items 14, 15, 16 and 17 amend existing section 49 of the Privacy Act, to ensure that, if the Commissioner refers a possible contravention of subsection 16E(1) to the Commissioner of Police or Director of Public Prosecutions, any investigation by the Commissioner into whether the conduct was also a possible contravention of the civil penalty provision must cease until such point (if any) where the Commissioner of Police or Director of Public Prosecutions advises the Commissioner that the matter will not be, or will no longer be, subject to proceedings for a criminal offence. These provisions together ensure that the imposition of both criminal and civil penalties for the same conduct will not result in entities being punished twice for the same conduct.

Section 16F Entity must notify responsible agency if de-identified personal information is re-identified

71. This section provides that an entity must notify a responsible agency if de-identified personal information is re-identified and is intended to ensure that when an entity re-identifies de-identified personal information, either intentionally or unintentionally, the responsible agency is informed by the entity of the re-identification whereupon the
the responsible agency must notify the Commissioner of what has occurred and may give the entity directions for dealing with the information.

72. Subsection 16F(1) provides that section 16F applies if:

- information has been published by, or on behalf of, an agency (the responsible agency) in a generally available publication (paragraph 16F(1)(a)); and

- the information was published on the basis that it was de-identified personal information (paragraph 16F(1)(b)); and

- on or after 29 September 2016, the entity does an act that has the result that the information is no longer de identified (paragraph 16F(1)(c)); and

- the entity becomes aware that the information is no longer de-identified (paragraph 16F(1)(d)).

73. An entity is defined by subsection 6(1) of the Privacy Act to include an agency, organisation or small business operator. This means that small business operators are subject to section 16F. Small business operators are generally excluded from the operation of the Privacy Act through the combined operation of subsection 6C(1), and sections 6D and 6DA of the Privacy Act. Small businesses operators are included in the scope of section 16F, including the civil penalty provisions of subsection 16E(4), (5) and (10), due to the need for a general deterrent to the re-identification of de identified personal information, rather than a deterrent limited to entities subject to the Privacy Act, which would otherwise generally exclude small business operators.

74. Paragraph 16F(1)(a) means that de-identified personal information must be contained in a generally available publication rather than disclosed in other more limited circumstances by the responsible agency. The term ‘generally available publication’ is defined in subsection 6(1) of the Privacy Act to mean a publication that is, or will be, generally available to the public, whether or not it is published in print, electronically, or in any other form, and whether or not it is available on the payment of a fee.

75. The reference to information that ‘was published on the basis it was de-identified personal information’ in subsection 16F(1)(b) is intended to convey that the section applies where an agency intended the published information to be de-identified information, regardless of whether it was possible to re-identify the information. ‘De-identified’ is defined in subsection 6(1) of the Privacy Act to mean that information is not ‘de-identified’ where it is no longer about an identifiable or reasonably identifiable individual. This definition accords with the definition of ‘personal information’ in subsection 6(1), which (in short) is information about ‘an identifiable or reasonably identifiable individual’.

76. Though an agency which publishes inadequately de-identified personal information will not breach any provision of the Bill, the agency would nonetheless risk breaching existing provisions of the APPs in the Privacy Act which regulate handling, disclosure and access to personal information. The Bill also provides the Commissioner with additional
assessment powers to ensure appropriate independent oversight applies to agency de-identification activities (see Item 6 below).

77. Circumstances of disclosure that would not fall under subsection 16F(1) could include, for example, disclosure under agreement by the responsible agency to a service provider for the provision of a service or to a researcher or research institution for research purposes. The provision in paragraph 16F(1)(a) that the information may also be published on behalf of an agency anticipates that if the responsible agency uses another party to publish the information in a generally available publication, then the re-identification by an entity of this information should also contravene subsection 16F(1).

78. Paragraph 16F(1)(c) provides that an entity must have done an act that has the result of achieving the de-identification of the information. As a result, information that is de-identified intentionally and unintentionally is subject to paragraph 16F(1)(c) as provided for in subsection 16F(2) of the Bill. Paragraph 16F(1)(c) applies retrospectively to an act by an entity on or after 29 September 2016 that has the result that the information is no longer de-identified. This retrospectivity is necessary because releases of private information can have significant consequences for individuals beyond their privacy and reputation, which cannot be easily remedied. In addition, the retrospective commencement of the offences creates a strong disincentive for entities to engage in such conduct while the Parliament considers the Bill.

79. Paragraph 16F(1)(d) provides that an entity must be aware that the information is no longer de-identified. This will mean that if the entity is not aware the information is no longer de-identified it will not contravene subsection 16F(1).

80. Subsection 16F(2) provides that paragraph 16F(1)(c) applies regardless of whether the entity intended to do the act or whether the entity intended the act to have the result that the information is no longer de-identified.

81. Subsection 16F(3) provides that as soon as practicable after becoming aware that the information is no longer de-identified, the entity must notify the responsible agency in writing of the fact. This notification will enable the responsible agency to take any steps necessary to respond to the de-identification. This may include, for example, the removal of the dataset from general availability in order to address any de-identification issues, or the removal of other datasets which rely on similar or the same de-identification techniques. Although section 16F applies to an act by an entity that has the result that the information is no longer de-identified on or after September 2016, the requirement to notify the Commissioner as soon as practicable in subsection 16F(3) will only apply from commencement (see Item 21 below).

82. Subsection 16F(4) provides that the entity must not use the information, or disclose the information to a person or entity other than the responsible agency after becoming aware that the information is no longer de-identified.

83. Subsections 16F(3) and (4) provide that, if contravened, an entity is liable to a civil penalty of 200 penalty units. Relevantly, the civil penalty provisions in subsections 16F(2) and (3) are set at a lower level than sections 16D and 16E of the Bill and contain no criminal
offence provisions. This reflects that section 16F also captures unintentional re-identification, which should not attract criminal penalties or civil penalties equivalent to those which apply under sections 16D and 16E. As with civil penalties under sections 16D and 16E, it is also intended that the upper limit of civil penalties under section 16F would apply only in particularly serious cases where the entity has failed to comply with section 16F (for example, if the entity is aware that it has unintentionally re-identified health information but then fails to notify the responsible agency that the information is vulnerable to re-identification).

84. Subsection 16F(5) provides that subsections 16F(3) and (4) do not apply if the entity is an agency and the act was done in connection with the performance of the agency’s functions or activities; or was required or authorised to be done by or under an Australian law or a court/tribunal order. The exemption of agencies from contravention of subsections 16F(3) and (4) and therefore from their civil penalty provisions is justified as it will ensure agencies do not contravene subsections 16F(3) and (4) when engaging in their ordinary functions and activities such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

85. Subsection 16F(6) provides that subsections 16F(3) and (4) do not apply if the entity is a contracted service provider for a Commonwealth contract to provide services to the responsible agency and the act was done for the purposes of meeting (directly or indirectly) an obligation under the contract. The exemption of such entities from contravention of subsections 16F(3) and (4) and therefore from their civil penalty provisions is justified as it will ensure these entities do not contravene subsections 16F(3) and (4) when engaging in functions and activities for which they are contracted such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

86. Subsection 16F(7) provides that subsections 16F(3) and (4) do not apply if the entity has entered into an agreement with the responsible agency to perform functions or activities on behalf of the agency and the act was done in accordance with the agreement. Subsection 16F(6) is intended to apply in situations where an agency and an entity have a formal relationship of some kind that falls short of a contractual relationship of the kind that would be covered under subsection 16F(6) above. The exemption of such entities from contravention of subsections 16F(3) and (4) and therefore from their civil penalty provisions is justified as it will ensure these entities do not contravene subsections 16F(3) and (4) when engaging in functions and activities which they have entered an agreement for such as by matching a de-identified dataset to another dataset, or decryption activities to test information security.

87. Subsection 16F(8) provides that subsections 16F(3) and (4) do not apply if the entity is an exempt entity for the purposes of section 16F in accordance with a determination in force under section 16G of the Bill; and the act was done for a purpose specified in that determination in relation to the entity and in compliance with any condition specified in the determination. Section 16G of the Bill provides that the Minister may make an entity exempt from section 16F if the Minister is satisfied it is in the public interest to do so.
88. Subsection 16F(9) provides that a responsible agency may give directions to entities and must notify the Commissioner.

89. Paragraph 16F(9)(a) provides that the agency may give the entity written instructions for dealing with the information. It is expected that this may include, for example, information on the appropriate handling and/or destruction of the re-identified information.

90. Paragraph 16F(9)(b) provides that the agency must, as soon as practicable after being notified, give the Commissioner a written notice explaining what has occurred in relation to the information.

91. Subsection 16F(10) provides that an entity given a direction under paragraph 16F(9)(a) must comply with the direction. The subsection provides a civil penalty of 200 penalty units for failure to comply.

**Section 16G Minister may determine that entity is an exempt entity for certain purposes**

92. Section 16G provides a power for the Minister to determine that an entity is an exempt entity for the purposes of sections 16D, 16E or 16F. The intention of this power is to provide a mechanism by which entities engaging in valuable research in areas such as testing the effectiveness of de-identification techniques, cryptology or information security (which may involve the re-identification of de-identified information) can be granted an exemption from sections 16D, 16E or 16F so that this legitimate research may continue.

93. Subsection 16G(1) provides that the Minister may, if satisfied it is in the public interest, determine that an entity, or an entity included in a class of entities, is exempt for the purposes of sections 16D, 16E or 16F in relation to one or more specified purposes. The note to subsection 16G(1) clarifies that the Minister may revoke or vary such a determination under subsection 33(3) of the Acts Interpretation Act 1901.

94. Subsection 16G(2) lists the purposes which a determination made under subsection 16G(1) may specify. Specific research purposes involving cryptology, information security and data analysis are identified in paragraphs 16G(2)(a) to (c) and paragraph 16G(2)(d) provides a general ground for any other purpose the Minister considers appropriate. While it is expected that the predominant reason for an exemption determination under subsection 16G(1) will be in relation to the specific research purposes identified in subsection 16G(2), paragraph 16G(2)(d) ensures that the determination power will be available in the event that a different legitimate purpose for re-identifying information or disclosing re-identified information arises in the future.

95. Subsection 16G(3) provides that a determination made under subsection 16G(1) may be made subject to any conditions specified in the determination. For example, a determination may provide that a particular entity is exempt from sections 16D and 16E in relation to acts done for the purposes of research involving cryptology, but only in relation to two specific datasets. Where a determination is subject to a particular condition, the entity’s conduct must comply with that condition in order for the exemption in subsections 16D(5), 16E(6) or 16F(8) to apply.
96. Subsection 16G(4) provides that the Minister must consult the Commissioner before making a determination under subsection 16G(1).

97. Subsection 16G(5) provides that a determination made under subsection 16G(1) is a legislative instrument, but is exempt from section 42 (disallowance) of the Legislation Act 2003 (the Legislation Act). It is necessary to exempt determinations under subsection 16G(1) from the disallowance scheme in the Legislation Act, to provide certainty about the application of the law and to provide commercial certainty to entities. It is expected that in most cases the types of entities who may be suitable for exemption by a determination under subsection 16G(1) would be undertaking particular projects or research activities over a period of time involving research into encryption or information security. Generally these projects would involve a commercial benefit of some kind and would require the commitment of resources to undertake from the outset.

98. Where this research involves, for example, the re-identification of de-identified information or attempting to do so, such entities would commit criminal offences under sections 16D and 16E in the course of their research in the absence of any exemption. If determinations made under subsection 16G(1) were subject to disallowance, these entities could not be certain from the outset of a particular project that they will be able to complete the project. This is because if the determination was disallowed, from that point in time the entity would no longer be exempted from sections 16D or 16E, and would not be able to complete the project without the potential of committing an offence. In addition, it may be difficult for the entity to cease those particular research activities at the point of disallowance.

99. In order to avoid this, the entity would need to wait until the full disallowance period had expired to be sure that they would not be committing criminal offences in the course of their project or research. This would generally not be practical, as particular research projects may be subject to specific timeframes and, depending on when a determination is made, the disallowance period can be as long as 4-5 months.

100. In addition to the commercial uncertainty, legitimate research into encryption and information security which supports important public interest objects can be time critical. For example, it would not be desirable that an entity has to wait a lengthy period of time before being able to test the effectiveness of de-identification techniques, because if there are vulnerabilities in the techniques these could be exploited in the interim.

101. As determinations under subsection 16G(1) are legislative instruments, there remain appropriate safeguards through the requirement to table determinations before Parliament, the consultation requirements in section 17 of the Legislation Act and registration of any determination on the Federal Register of Legislation. In addition, the Minister must consult with the Commissioner prior to making any determination, which provides an additional degree of scrutiny and transparency.

Item 6 At the end of subsection 33C(1)

102. This item adds a new paragraph at the end of subsection 33C(1) to provide the Commissioner with the ability to conduct an assessment of whether methods used by agencies for de-identifying personal information are effective to protect individuals from
being identifiable or reasonably identifiable. This ability will complement the other measures in this Bill and existing assessment provisions in section 33 by providing independent oversight of agency de-identification practices. This will further encourage agencies to adopt best practice de-identification techniques and minimise the risk of published de-identified information being vulnerable to re-identification.

Item 7 Section 36A

103. This item amends part of the guide to Part V of the Privacy Act in section 36A to reflect amendments made to the investigation powers of the Commissioner by this Bill.

Item 8 Section 36A

104. This item corrects a minor typographical error in the Guide to Part V of the Privacy Act in section 36A by replacing ‘range powers’ with ‘range of powers’.

Item 9 Section 36A

105. This item amends part of the guide to Part V of the Privacy Act in section 36A to reflect amendments made to the investigation powers of the Commissioner by this Bill.

Item 10 After subsection 40(2)

106. This item inserts a new subsection in section 40, subsection 40(2A), which provides that the Commissioner may, on his or her own initiative, investigate an act that may contravene subsection 16D(1) or 16E(1) or 16F(3), (4) or (10). Paragraphs 40(2A)(a) and (b) provide the Commissioner may do so if he or she has received a notice under paragraph 16F(9)(b) or otherwise becomes aware that an entity may have contravened one of those subsections.

107. This limited investigation power for the Commissioner supports the Commissioner’s existing power to seek civil penalty orders in relation to civil penalty offences under Part VIB of the Privacy Act. A new own motion investigation power has been included rather than using existing investigation powers, given that the existing powers in section 40 either:

- are triggered by complaints from individuals about conduct which might be an ‘interference with the privacy of an individual’ (as defined in existing subsection 6(1) of the Privacy Act), or

- deal with Commissioner-initiated investigations into contraventions that are either an interference with the privacy of an individual or that breach existing APP 1 of the Privacy Act.

108. The existing Privacy Act complaints mechanism about conduct that might be an ‘interference with the privacy of an individual’ is not relevant to the new Division 3 of Part III given that a contravention of the Division is not taken to be an interference with the privacy of an individual. (This is because doing so would give rise to a range of enforcement powers which were designed to regulate enforcement of the APPs and other existing
provisions of the Privacy Act, and would not be appropriate for the scheme contained in the new Division 3 of Part III, which also applies, for example, to individuals acting in their personal capacity and small businesses who would otherwise be exempt from the Privacy Act.) This would not, however, prevent the Commissioner from commencing an investigation under section 40(2A) after an individual brings a possible contravention of subsection 16D(1) or 16E(1) or 16F(3), (4) or (10) to the Commissioner’s attention.

**Item 11 At the end of subsection 42(2)**

109. This item inserts ‘or (2A)’ at the end of subsection 42(2). This amendment is consequential to the amendment in item 10 above and ensures that the Commissioner’s ability to make preliminary enquires applies in relation to investigations under new subsection 40(2A).

**Item 12 Subsection 43(1AA)**

110. This item inserts ‘or (2A)’ after ‘subsection 40(2)’ in subsection 43(1AA). This amendment is consequential to the amendment in item 10 above and ensures that the requirement for the Commissioner to inform an entity that the Commissioner is about to conduct an investigation into that entity’s act or practice applies to investigations under new subsection 40(2A).

**Item 13 Subsection 43A(1)**

111. This item amends subsection 43A(1) to insert the words ‘(other than under subsection 40(2A))’. This amendment makes clear that an interested party in relation to an investigation under new subsection 40(2A) cannot request the Commissioner to hold a hearing (as the Commissioner would not be able to make a determination under section 52 in relation to the investigation). A formal hearing mechanism is not considered necessary for investigations under subsection 40(2A) given the limited possible ways in which such an investigation might conclude (see Item 19 below) compared to the wider range of options available to the Commissioner when closing investigations through a determination under section 52. It is nonetheless expected that the Commissioner would conduct investigations in accordance with usual standards of natural justice and procedural fairness to ensure entities are able to adequately make representations to the Commissioner during the course of an investigation under subsection 40(2A).

**Item 14 Subsection 49(1)**

112. This item amends subsection 49(1) to insert ‘a re-identification offence’. This extends the existing requirement for the Commissioner to inform the Commissioner of Police or the Director of Public Prosecutions when he or she forms the opinion that certain offences may have been committed to the new offences under sections 16D or 16E.
Item 15  At the end of paragraph 49(1)(a)

113. This item inserts the word ‘and’ at the end of paragraph 49(1)(a). This minor technical amendment clarifies the operation of subsection 49(1) and is consistent with the Office of Parliamentary Counsel’s drafting conventions.

Item 16  After paragraph 49(1)(b)

114. This item inserts new paragraph 49(1)(ba) into subsection 49(1). This paragraph requires the Commissioner to provide all relevant information to the Commissioner of Police or the Director of Public Prosecutions regarding an investigation under subsection 40(2A). This is equivalent to the existing requirement in paragraph 49(1)(b) in relation to investigations under subsection 40(1).

Item 17  Subsection 49(4)

115. This item inserts the definition of ‘re-identification offence’ in subsection 49(4). ‘Re-identification offence’ is defined as an offence against subsection 16D(6) or 16E(7) or the related offences against section 6 of the Crimes Act 1914 or sections 11.1, 11.2, 11.4 or 11.5 of the Criminal Code. This amendment supports the amendment in item 14 above, which inserts ‘re-identification offence’ into subsection 49(1).

Item 18  Section 52 (heading)

116. This item repeals the heading for section 52 and substitutes a new heading ‘Determination of the Commissioner—investigations other than in relation to re-identified personal information’. This amendment is consequential to the amendment in item 19, which provides for a separate determination power in relation to investigations under new subsection 40(2A).

Item 19  After section 53

117. This item inserts new section 53AA, which provides that the Commissioner may make a written determination following an investigation under subsection 40(2A) that it would be inappropriate for any further action to be taken in relation to the matter. New subsection 53AA(2) provides that where the Commissioner makes such a determination, he or she must notify the entity who is subject to the investigation that no further action is to be taken in relation to the matter.

118. The determination power in new section 53AA is in addition to the existing determination power in section 52 of the Privacy Act. Section 52 provides the Commissioner with power to make determinations in a range of forms as the Commissioner sees fit, and a determination under section 52 triggers a range of review and enforcement mechanisms in Divisions 2, 3 and 4 of Part V.

119. In the case of an investigation under subsection 40(2A), however, the only expected outcome of the investigation is that the Commissioner will either:
- take no further action because the entity has been convicted of a criminal offence for conduct that also falls under a civil penalty provision in section 16D or 16E,
- apply to the Federal Court or Federal Circuit Court to impose a civil penalty for a contravention of 16D(1) or 16E(1) where criminal proceedings will not or cannot proceed, or where the entity has contravened subsections 16F(3), (4) or (10), or
- make a determination to close the investigation, where neither of the above options apply.

120. Therefore, given the limited effect of a determination closing an investigation under subsection 40(2A) compared to determinations under section 52, and the fact that there would be no utility in making the former kind of determination enforceable or reviewable, a distinct determination power has been included in new section 53AA rather than merely expanding the existing power in section 52.

**Item 20 Application of amendments**

121. This item provides that paragraphs 16D(1)(a), 16E(1)(a) and 16F(1)(a) apply in relation to information that was published by, or on behalf of, an agency before or after the commencement of this item.

**Item 21 Transitional—obligations of entities in relation to information that was re-identified on or after 29 September 2016 and before commencement**

122. This item provides for transitional arrangements regarding the application of new section 16F in relation to information that was re-identified on or after 29 September 2016 and before commencement.

123. Sub-item 21(1) provides that the item applies where new subsection 16F(1) applies in relation to information and an entity, and the entity had become aware before the commencement of this item that the information was no longer de-identified.

124. Sub-item 21(2) provides that subsection 16F(3) applies in relation to the entity as if that subsection required the entity to notify the responsible agency as soon as practicable after the commencement of this item that the information is no longer de-identified. This ensures that the obligation to notify an agency in relation to re-identified information does not exist for an entity until commencement where that re-identification occurred on or after 29 September 2016 and before commencement.

125. Sub-item 21(3) provides that subsection 16F(4) applies in relation to the entity after the commencement of this item. This item clarifies that while the obligation in subsection 16F(4) may relate to information re-identified on or after 29 September 2016 and before commencement, the obligation in subsection 16F(4) does not apply retrospectively.
Part 2—Other amendments

*Australian Information Commissioner Act 2010*

**Item 22  Paragraph 25(l)**

126. This item amends paragraph 25(l) of the *Australian Information Commissioner Act 2010* to insert the words ‘or 53AA’ after ‘section 52’. This amendment is consequential to the amendment in item 19 above which provides for a separate determination power in relation to investigations under new subsection 40(2A). This ensures that power to make determinations under section 53AA is treated consistently with determinations under section 52, which the Australian Information Commissioner Act provides in paragraph 25(l) cannot be delegated by the Commissioner.