2013-2014-2015

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES/THE SENATE

PRIVACY AMENDMENT (NOTIFICATION OF SERIOUS DATA BREACHES) BILL 2015

EXPLANATORY MEMORANDUM

(Circulated by authority of the

Attorney-General, Senator the Hon George Brandis QC)

PRIVACY AMENDMENT (NOTIFICATION OF SERIOUS DATA BREACHES) BILL 2015

GENERAL OUTLINE

1. This Bill amends the *Privacy Act 1988* (**the Privacy Act**) to introduce mandatory data breach notification provisions for agencies, organisations and certain other entities that are regulated by the Privacy Act (**entities**). The Bill will commence on a single day fixed by proclamation. However, if the provisions do not commence before 12 months from the day after the Bill receives the Royal Assent, they will commence on that day.

2. Mandatory data breach notification commonly refers to a legal requirement to provide notice to affected individuals and the relevant regulator when certain kinds of security incidents compromise information of a certain kind or kinds. In some jurisdictions, notification is also only required if the data breach meets a specified harm threshold. Examples of when data breach notification may be required could include a malicious breach of the secure storage and handling of information (e.g. in a cyber security incident), an accidental loss (most commonly of IT equipment or hard copy documents), a negligent or improper disclosure of information, or otherwise, where the incident satisfies the applicable harm threshold (if any).

3. In its Report 108, *For Your Information: Australian Privacy Law and Practice*, the Australian Law Reform Commission (**ALRC**) noted that, with advances in technology, entities were increasingly holding larger amounts of personal information in electronic form, raising the risk that a security breach around this information could result in others using the information for identity theft and identity fraud. A notification requirement on entities that suffer data breaches will allow individuals whose personal information has been compromised by a breach to take remedial steps to lessen the adverse impact that might arise from the breach. For example, the individual may wish to change passwords or take other steps to protect his or her personal information.

4. The ALRC recommended that the Privacy Act be amended to require that such notification be given. Under the ALRC's proposed test, notification would be provided to those whose privacy had been infringed when data breaches causing 'a real risk of serious harm' occurred. Notification would be compulsory unless it would impact upon a law enforcement investigation or was determined by the regulator to be contrary to the public interest.

5. In February 2015, the advisory report of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 also recommended the introduction of a mandatory data breach notification scheme by the end of 2015. The Government's response to the PJCIS report in March 2015 agreed to this recommendation.

6. This Bill implements the recommendations of the ALRC and the PJCIS by requiring agencies and organisations regulated by the Privacy Act to provide notice to the Australian Information Commissioner (**the Commissioner**) and affected individuals of a serious data breach. The Bill contains general rules for the majority of entities regulated by the Privacy Act as well as analogous rules for credit reporting bodies and credit providers that are subject to specific regulation under Part IIIA, which deals with consumer credit reporting. The

provisions in the Bill also apply to recipients of tax file number information. Each type of entity is subject to common requirements under the Privacy Act to protect the types of personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

7. A data breach arises where there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals, or where such information is lost in circumstances that are likely to give rise to unauthorised access or unauthorised disclosure. A data breach is a serious data breach where there is a *real risk of serious harm to the individual* to whom the information relates as a result of the data breach **(the affected individual)**. This is based on the standard recommended by the ALRC and also incorporated in the current voluntary data breach guidelines issued by the Office of the Australian Information Commissioner **(OAIC)**. In addition, the Bill provides for regulations to specify particular situations that may also be serious data breaches even if they do not necessarily reach the threshold of a real risk of serious harm. For example, this could include the release of particularly sensitive information such as health records which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection.

8. Serious harm, in this context, includes physical, psychological, emotional, economic and financial harm, as well as harm to reputation. The risk of harm must be real, that is, not remote, for it to give rise to a serious data breach. It is not intended that every data breach be subject to a notification requirement. It would not be appropriate for minor breaches to be notified because of the administrative burden that may place on entities, the risk of 'notification fatigue' on the part of individuals, and the lack of utility where notification does not facilitate harm mitigation.

9. In the event of a serious data breach, the regulated entity is required to notify the Commissioner and affected individuals as soon as practicable after the entity is aware, or ought reasonably to have been aware, that there are reasonable grounds to believe that there has been a serious data breach. The notification must include:

- the identity and contact details of the entity
- a description of the serious data breach
- the kinds of information concerned, and
- recommendations about the steps that individuals should take in response to the serious data breach.

10. When providing the information described above to affected individuals, the entity may use the method of communication (if any) that it normally uses to communicate with the individual. This is designed to reduce the cost of compliance for entities, and also to ensure that individuals trust and act upon the information provided. Information received from an entity using a different method of communication may be dismissed as a scam resulting in individuals failing to take steps to mitigate harm arising from a serious data breach. Where there is no normal mode of communication with the particular individual, the entity must take

reasonable steps to communicate with them. Reasonable steps could include making contact by email, telephone or post.

11. There may be circumstances in which it is impracticable to provide a notification to each affected individual. The Bill provides that, in these circumstances, an entity will not be required to provide notice directly to each affected individual but will rather be required to provide the information described above on its website (if any) and to take reasonable steps to publicise the information.

12. Not all entities will be subject to the data breach notification requirement. Those entities already exempt from the operation of the Privacy Act in whole or in part, such as intelligence agencies and small business operators, will enjoy the same exemption in relation to the measures in this Bill. Law enforcement bodies will not be required to notify affected individuals if compliance with this requirement would be likely to prejudice law enforcement activities.

13. Further exceptions to the data breach notification requirement may apply to other entities that are subject to the operation of the Privacy Act. If compliance would be inconsistent with another law of the Commonwealth that regulates the use or disclosure of information, an entity will be exempt to the extent of the inconsistency. Entities will also be exempt from notifying a serious data breach that falls under the mandatory data breach notification requirement in section 75 of the *My Health Records Act 2012* (**the My Health Records Act**). Entities will also be exempt if, after becoming aware that there are reasonable grounds to believe a serious data breach has occurred, the entity subsequently carries out a reasonable assessment of the circumstances within 30 days which finds that there are in fact not reasonable grounds to believe a serious data breach occurred.

14. In addition, the Commissioner may exempt an entity from providing notification of a serious data breach where the Commissioner is satisfied that it is in the public interest to do so. The Commissioner may issue an exemption on application from an entity or on the Commissioner's own initiative.

15. In circumstances where the Commissioner believes that a serious data breach has occurred and no notification has been given by the entity that suffered the breach, the Commissioner may issue a written direction to the entity requiring it to provide notification of the data breach. The information to be provided to the Commissioner and affected individuals will be the same as if the entity had initiated the notification itself, with the exception that the Commissioner may also require the entity to provide other information about the serious data breach that the Commissioner considers appropriate in the circumstances. Similarly, the requirements as to communicating with individuals will be the same. A law enforcement body that reasonably believes that compliance with the Commissioner's direction would be likely to prejudice law enforcement activities will be exempt from complying with the direction. An entity would also be exempt from complying with the direction to the extent that compliance would be inconsistent with another law of the Commonwealth that regulates the use and disclosure of information. The Commissioner will also be required not to issue a direction in relation to a serious data breach if the breach falls

under the mandatory data breach notification requirement in section 75 of the My Health Records Act.

16. Failure to comply with an obligation included in the Bill will be deemed to be an interference with the privacy of an individual for the purposes of the Privacy Act. This will engage the Commissioner's existing powers to investigate, make determinations and provide remedies in relation to non-compliance with the Privacy Act. This includes the capacity to undertake Commissioner initiated investigations, make determinations, seek enforceable undertakings, and pursue civil penalties for serious or repeated interferences with privacy.

17. This approach will permit the use of less severe sanctions before elevating to a civil penalty. These less severe penalties could include public or personal apologies, compensation payments or enforceable undertakings. A civil penalty would only be applicable where there has been a serious or repeated non-compliance with mandatory notification requirements. Civil penalties would be imposed by the Federal Court or Federal Circuit Court on application by the Commissioner.

18. A decision by the Commissioner to refuse to grant an exemption in response to an application from the entity or to give a direction that an entity provide notification of a serious data breach will be reviewable by the Administrative Appeals Tribunal.

19. It is anticipated that the Commissioner will update the current OAIC *Data Breach Notification: A guide to handling personal information security breaches* or release other guidance material to reflect the passage of this Bill and to assist entities in preventing, identifying, notifying and containing serious data breaches.

FINANCIAL IMPACT STATEMENT

20. [Statement to be inserted at a later date.]

REGULATION IMPACT STATEMENT

[Draft Regulation Impact Statement to be published separately to this Exposure Draft Bill.]

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

[Statement to be inserted at a later date.]

NOTES ON CLAUSES

Preliminary

Clause 1—Short title

1. This clause provides that when the Bill is enacted, it may be cited as the *Privacy Amendment (Notification of Serious Data Breaches) Act 2015*.

Clause 2—Commencement

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

3. 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 a single day fixed by proclamation. However, if the provisions do not commence before 12 months from the day after the Bill receives the Royal Assent, they will commence on that day.

4. 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

5. 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

Privacy Act 1988

Item 1 Subsection 6(1)

6. Item 1 of Schedule 1 inserts a definition of 'serious data breach' into existing subsection 6(1) of the Privacy Act. This Item provides that the term 'serious data breach' has the meaning given by section 26WB, which is inserted into the Privacy Act by this Bill (see Item 3, below).

7. This definition is intended to capture data breaches that are significant enough to warrant notification. This will ensure the Government does not create or impose an unreasonable compliance burden on entities regulated by the scheme, and avoid the risk of

'notification fatigue' among individuals receiving a large number of notifications in relation to non-serious breaches.

Item 2 After subsection 13(4)

8. Item 2 of Schedule 1 inserts a new subsection 13(4A) into the Privacy Act after subsection 13(4). New subsection 13(4A) is titled 'Notification of serious data breaches', and provides that if an entity (within the meaning of Part IIIC) contravenes either new section 26WC or 26WD of the Privacy Act (which are inserted by this Bill), the contravention is taken to be an act that is an 'interference with the privacy of an individual'. Subsection 6(1) of the Privacy Act provides that the term 'interference with the privacy of an individual' has the meaning given by sections 13 to 13F of the Privacy Act.

9. The effect of new subsection 13(4A) of the Privacy Act will be to enable the Australian Information Commissioner (**the Commissioner**) to use the powers and access the remedies available to the Commissioner under the Privacy Act to investigate and address contraventions of section 26WC or 26WD. These include the capacity for the Commissioner to initiate investigations, make determinations, seek enforceable undertakings, and make applications for civil penalties for serious or repeated interferences with privacy.

10. A civil penalty for serious or repeated interferences with the privacy of an individual will only be issued by the Federal Court or Federal Circuit Court of Australia following an application by the Commissioner. Serious or repeated interferences with the privacy of an individual attract a maximum penalty of 2,000 penalty units for individuals and 10,000 penalty units for bodies corporate.

11. The Commissioner also has guidance related functions under paragraph 28(1)(a) of the Privacy Act to make guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals. The Commissioner will consequently have the discretion to issue guidelines under paragraph 28(1)(a) about matters relating to compliance with the new Part IIIC—Notification of serious data breaches.

Item 3 After Part IIIB

12. Item 3 of Schedule 1 inserts a new Part IIIC, titled 'Notification of serious data breaches', into the Privacy Act following existing Part IIIB. This new Part contains the substantive elements of the mandatory data breach notification provisions, which apply to entities that are regulated by the Privacy Act.

13. The Part is divided into four Divisions. Broadly, the first Division sets out a simplified outline of the Part, the second Division sets out when a 'serious data breach' will have occurred, the third Division contains obligations for entities to notify serious data breaches, subject to limited exceptions, and the fourth Division defines key terms used in the Part.

Division 1—Introduction

Section 26WA Simplified outline of this Part

14. New section 26WA sets out a brief outline to the contents of Part IIIC—Notification of serious data breaches. The outline explains the purpose of the Part, what constitutes a serious data breach and when an entity must notify a serious data breach.

Division 2—Serious data breach

Section 26WB Serious data breach

15. This section sets out the circumstances in which a 'serious data breach' occurs. In short, the section provides that a serious data breach occurs where:

- there is unauthorised access to, or unauthorised disclosure of specified kinds of information held by specified entities about one or more individuals, or loss of that information that is likely to lead to unauthorised access or unauthorised disclosure of the information, and

- as a result, there is or would be a 'real risk of serious harm' to any of the individuals to whom the information relates.

16. The section also provides that, where specified entities holds specified kinds of information about one or more individuals, a serious data breach occurs where:

- there is unauthorised access to, or unauthorised disclosure of, information of a kind specified in the regulations, or

- there is loss of information of a kind specified in the regulations, and unauthorised access to or unauthorised disclosure of the information may occur as a result.

Scope

17. New subsection 26WB(1), which is titled 'Scope', sets out the kinds of entities and information which a data breach must involve to satisfy the definition of a 'serious data breach'. Each kind of entity included in the subsection is already subject to the Privacy Act. The subsection also provides that a serious data breach can only occur in relation to information that is subject to existing Privacy Act security requirements.

18. Paragraph 26WB(1)(a) provides that section 26WB applies if:

- an APP entity holds personal information relating to one or more individuals (subparagraph 26WB(1)(a)(i)), and

- the APP entity is required under section 15 of the Privacy Act not to do an act, or engage in a practice that breaches Australian Privacy Principle (**APP**) 11.1 of the Privacy Act in relation to the information (subparagraph 26WB(1)(a)(ii)).

19. ‘Personal information’ is defined in subsection 6(1) of the Privacy Act to include information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. ‘APP entity’ is defined in subsection 6(1) of the Privacy Act to include Commonwealth government agencies and private sector organisations regulated by the Privacy Act. APP 11.1 of the Privacy Act requires APP entities to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

20. Paragraph 26WB(1)(b) provides that section 26WB applies if:

- a credit reporting body holds credit reporting information relating to one or more individuals (subparagraph 26WB(1)(b)(i)), and
- the credit reporting body is required to comply with section 20Q of the Privacy Act in relation to the information (subparagraph 26WB(1)(b)(ii)).

21. ‘Credit reporting information’ is defined in subsection 6(1) of the Privacy Act and includes the credit-related information about individuals collected by credit providers. ‘Credit reporting body’ is defined in subsection 6(1) of the Privacy Act as an organisation, or an agency prescribed by regulation, which carries on a credit reporting business. Section 20Q of the Privacy Act is based on APP 11.1 and requires credit reporting bodies to, among other things, protect credit reporting information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

22. Paragraph 26WB(1)(c) provides that section 26WB applies if:

- a credit provider holds credit eligibility information relating to one or more individuals (subparagraph 26WB(1)(c)(i)), and
- the credit provider is required to comply with subsection 21(S)(1) of the Privacy Act in relation to the credit reporting information (subparagraph 26WB(1)(c)(ii)).

23. ‘Credit eligibility information’ is defined in subsection 6(1) of the Privacy Act as including credit reporting information disclosed to a credit provider by a credit reporting body and information derived from the credit reporting information. ‘Credit provider’ is defined in section 6G of the Privacy Act as including a bank or other organisation that provides credit as a substantial part of its business or undertaking. Subsection 21S(1) of the Privacy Act is based on APP 11.1 and requires credit providers to protect credit eligibility information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

24. Paragraph 26WB(1)(d) provides that section 26WB applies if:

- a file number recipient holds tax file number information relating to one or more individuals (subparagraph 26WB(1)(d)(i)), and

- the file number recipient is required under section 18 of the Privacy Act not to do an act, or engage in a practice, that breaches a rule issued under section 17 of the Privacy Act that relates to the tax file number information (subparagraph 26WB(1)(d)(ii)).

25. 'Tax file number' and 'tax file number information' are defined in subsection 6(1) of the Privacy Act. 'File number recipient' is defined in section 11 of the Privacy Act to include a person who is (whether lawfully or unlawfully) in possession or control of a record that contains tax file number information. Section 17 of the Privacy Act provides that the Commissioner must issue rules concerning the collection, storage, use and security of tax file number information. Section 18 of the Privacy Act provides that a file number recipient shall not do an act, or engage in a practice, that breaches a rule issued under section 17.

Serious data breach

26. New subsection 26WB(2), which is titled 'Serious data breach', establishes the circumstances that will constitute a 'serious data breach' when information within scope of section 26WB is subject to unauthorised access, unauthorised disclosure or loss.

27. Paragraph 26WB(2)(a) provides that a serious data breach will occur in situations where unauthorised access to or unauthorised disclosure of information of a kind referred to in new subsection 26WB(1) occurs, and:

- the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the information relates (subparagraph 26WB(2)(a)(i)), or

- any of the information is of a kind specified in the regulations (subparagraph 26WB(2)(a)(ii)).

28. If subparagraph 26WB(2)(a)(ii) applies, unauthorised access to or unauthorised disclosure of information specified in the regulations is taken to be a serious data breach regardless of the risk of harm to individuals. This is intended to provide the flexibility to deal with data breaches that may not reach the threshold of a real risk of serious harm, but should nevertheless be subject to notification. These could include data breaches involving particularly sensitive information such as health records, which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection.

29. Paragraph 26WB(2)(b) provides that a serious data breach will occur in situations where information of a kind referred to in new subsection 26WB(1) is lost in circumstances where:

- unauthorised access to or unauthorised disclosure of the information is likely to occur (subparagraph 26WB(2)(b)(i)), and

- the access or disclosure, assuming it were to occur, will result in a real risk of serious harm to any of the individuals to whom the information relates (subparagraph 26WB(2)(b)(ii)).

30. In the context of subparagraph 26WB(2)(b)(i), the phrase 'likely' is intended to ensure that loss of information will not be considered a serious data breach if it is not probable that the information will be subject to unauthorised access or unauthorised disclosure as a result. Examples may include hardcopy information lost after it has been accidentally disposed of in a secure waste disposal, or the loss of an electronic storage device that has been encrypted or contains encrypted information where the probability of the encryption being circumvented is low.

31. Paragraph 26WB(2)(c) provides that a serious data breach will occur in situations where information of a kind referred to in new subsection 26WB(1) is lost in circumstances where:

- unauthorised access to or unauthorised disclosure of the information may occur (subparagraph 26WB(2)(c)(i)), and

- any of the information is of a kind specified in the regulations (subparagraph 26WB(2)(c)(ii)).

32. Similar to subparagraph 26WB(2)(a)(ii) above, paragraph 26WB(2)(c) is intended to provide the flexibility to deal with data breaches where loss of particularly sensitive information may result in unauthorised access or unauthorised disclosure. Paragraph 26WB(2)(c) would apply regardless of the likelihood of such access or disclosure actually occurring following the loss, and regardless of the risk of harm that would occur as a result. This again recognises that particularly sensitive information should be subject to the highest level of privacy protection.

33. In the context of the new Part IIIC—Notification of serious data breaches, 'serious harm' includes physical, psychological, emotional, economic and financial harm, as well as harm to reputation (new section 26WF). To give rise to a serious data breach, the risk of harm must be real (that is, not remote) (new section 26WG) and the harm must be of a serious nature. In order not to impose an unreasonable compliance burden on entities and to avoid the risk of 'notification fatigue' among individuals receiving a large number of notifications in relation to non-serious breaches, it is not intended that every data breach be subject to a notification requirement.

34. This Item also inserts two Notes following new subsection 26WB(2) and before new subsection 26WB(3). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26WF. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26WG.

Relevant matters

35. New subsection 26WB(3), which is titled 'Relevant matters', provides a non-exhaustive list of matters entities must have regard to when determining whether a real risk of serious harm exists for the purposes of new subparagraphs 26WB(2)(a)(i) or 26WB(2)(b)(ii). Not all the matters listed will necessarily be particularly relevant in all circumstances. While in some cases one matter may be determinative in considering whether a real risk of serious

harm exists, in other cases, it may be that the entity or Commissioner also consider that a real risk of serious harm exists when the relevant matters are considered as a whole.

36. Most of the matters listed in new subsection 26WB(3) are based on matters identified in the current OAIC *Data Breach Notification: A guide to handling personal information security breaches*, or matters identified in the ALRC report.

37. The current OAIC *Data breach notification guide: A guide to handling personal information security breaches* and *Guide to securing personal information: 'Reasonable steps' to protect personal information* already provide advice about encryption and other security measures that are consistent with information security requirements in the Privacy Act. The Commissioner would have the discretion to expand or update this guidance to reflect the introduction of the new Part IIIC—Notification of serious data breaches, or to introduce specific security guidelines relating to Part IIIC. This could include guidance material about the matters in subsection 26WB(3) and the process of determining whether a real risk of serious harm exists for the purposes of new subparagraphs 26WB(2)(a)(i) or 26WB(2)(b)(ii).

38. Paragraph 26WB(3)(a) provides that the kind or kinds of information concerned in a data breach is a relevant matter when determining whether a real risk of serious harm exists. For example, a data breach involving an individuals' government-issued identifier (such as their Medicare number or driver's licence number) or financial details (such as their credit card details) might pose a greater risk of harm to the individual than a data breach involving only their name. Similarly, particular combinations of information (for example, a combination of name, address and date of birth) might pose a greater risk of harm than a single piece of information. However, in assessing whether there is a real risk of serious harm, it is relevant for an entity to consider whether a real risk of serious harm might be presented because the information could be combined with other information.

39. The permanence of a particular kind of information may be relevant when considering the kind of information concerned in a data breach. For example, an entity could potentially take action to mitigate the risk to an individual arising from a data breach involving information that can be re-issued, such as a compromised customer password, but cannot change 'permanent information' such as the individual's date of birth or medical history.

40. Paragraph 26WB(3)(b) provides that the sensitivity of the information is a relevant matter when determining whether a real risk of serious harm exists. Where sensitivity arises because of the kind of information involved, the associated issues will in some cases be similar or identical to those discussed under paragraph 26WB(3)(a) above, and it is expected that entities or the Commissioner will be able to consider the matters under paragraphs 26WB(3)(a) and (b) together.

41. In other cases the sensitivity of the information may relate to issues that are independent from the kind of information involved. An example would be an unauthorised disclosure of the names and addresses of individuals who are accessing a particular government service, or who are clientele of a particular business: although the data breach would involve information that would generally not be intrinsically sensitive, sensitivity may

nonetheless arise if the knowledge that the individual was accessing the service or was a client of the business could cause harm.

42. Paragraph 26WB(3)(c) provides that whether the information involved in a data breach is in a form that is intelligible to an ordinary person is a relevant matter when determining whether a real risk of serious harm exists. The phrasing is intended to be technology neutral, and could apply to either electronic or hardcopy information (although additional considerations apply in relation to electronic information: see new subsection 26WB(4) below).

43. Examples of information that may not be intelligible to an ordinary person depending on the circumstances include:

- encrypted electronic information
- information that the entity holding the information could likely use to identify an individual, but that other entities or individuals likely could not (an example would be information that the entity could link to a particular individual, but that would be 'de-identified information' to other entities or individuals)
- information that has been adequately destroyed as per APP 11.2 in the Privacy Act and cannot be retrieved to its original form (such as adequately shredded hard copy information).

44. The 'ordinary person' element of paragraph 26WB(3)(c) sets an objective standard based on whether the information would be intelligible to an ordinary person (see also subsection 26WB(4) below in relation to electronic information). The test is not intended to preclude consideration of whether the information would be intelligible to a person with knowledge or capabilities exceeding those of an ordinary person: in such a case other relevant matters listed in new subsection 26WB(3) may be relevant (in particular paragraphs 26WB(3)(e)–(g) below about security measures protecting the information and the persons or kinds of persons who have obtained, or could obtain, the information).

45. Paragraph 26WB(3)(d) provides that, if the information involved in a data breach is not in a form intelligible to an ordinary person, the likelihood that the information could be converted into such a form is a relevant matter when determining whether a real risk of serious harm exists. For example, encrypted information may not be intelligible to an ordinary person (as per paragraph 26WB(3)(c) above), but if the encryption method used could be circumvented—which could occur if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken by a sophisticated attacker, or if the decryption key was also accessed or disclosed in the data breach—the risk could exist that the information could be converted into a form intelligible to an ordinary person. Even where none of these concerns apply in relation to encrypted information, the entity may need to consider the likelihood of the encryption algorithm being broken in the long-term.

46. In the same way as paragraph 26WB(3)(c) above, the 'ordinary person' element of paragraph 26WB(3)(d) sets an objective standard that asks the entity to consider whether the information could be rendered in a form intelligible to an ordinary person (see also

subsection 26WB(4) below in relation to electronic information). Importantly, however, paragraph 26WB(3)(d) is not concerned with whether an ordinary person would themselves be capable of converting the information into a form that would be intelligible to such a person. The paragraph could still be particularly relevant even if converting the information into a form intelligible to an ordinary person would require knowledge or capabilities likely to exceed those of an ordinary person: it is the likelihood of such a conversion occurring which will influence whether a real risk of serious harm exists. Nor does paragraph 26WB(3)(d) preclude consideration of whether the information might be converted to a form that would be intelligible only to a person with knowledge or capabilities likely to exceed those of an ordinary person. If either of these considerations apply, other matters listed in new subsection 26WB(3) may be particularly relevant (in particular paragraphs 26WB(3)(e)–(g) below).

47. Paragraph 26WB(3)(e) provides that whether the information is protected by one or more security measures is a relevant matter when determining whether a real risk of serious harm exists. For example, if an entity's intrusion detection and prevention systems detect an attack on the entity's IT networks, the entity could consider whether network security mechanisms were likely to have prevented the attacker from accessing information falling under subsection 26WB(1).

48. In relation to electronic information, considerations that may apply under paragraph 26WB(3)(e) may be similar or identical to matters that may be relevant under paragraph 26WB(3)(c) above. But particularly in cases where an entity has reasonable grounds but not definitive proof to believe that unauthorised access to or unauthorised disclosure of information has occurred, consideration of security measures that were in place to protect the information may be of greater utility in assessing whether a serious data breach has occurred than consideration of the intelligibility of the information concerned to an ordinary person.

49. Paragraph 26WB(3)(f) provides that, if the information involved in a data breach is protected by one or more security measures, the likelihood that any of those security measures could be overcome is a relevant matter when determining whether a real risk of serious harm exists. Returning to the example mentioned in relation to paragraph 26WB(3)(e) above, the entity could consider the likelihood that the attacker might have overcome network security measures protecting personal information stored on the network. The likelihood of security measures being overcome may depend on matters dealt with in other paragraphs of new subsection 26WB(3) (in particular new paragraph 26WB(3)(g) below).

50. Paragraph 26WB(3)(g) provides that the persons, or the kinds of persons, who have obtained, or who could obtain the information involved in data breach is a relevant matter when determining whether a real risk of serious harm exists. For the purposes of paragraph 26WB(3)(g), access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party who may wish to cause harm to the individual to whom the information relates (for example, a person against whom the individual has a restraining order).

51. For example, if an entity mistakenly emails the personal information of one client to another client, and is confident that the recipient has deleted the information without using it or disclosing it to further parties, the risk of serious harm to the affected individual may be unlikely. Similar considerations would apply if an employee of an entity accesses information of a kind included in subsection 26WB(1) above without malicious intent but without authorisation, where the entity has taken steps to mitigate the risk of harm (see paragraph 26WB(3)(i) below) and continues to otherwise comply with the Privacy Act in relation to the information.

52. A contrasting example would be if information falling under new subsection 26WB(1) was exfiltrated from an entity's IT network in a cyber security incident. Paragraph 26WB(3)(g) may be particularly relevant in determining the risk of harm if the information was obtained, or could be obtained, by individuals with the capability and motive to use the information to cause serious harm to affected individuals (in these circumstances, paragraphs 26WB(3)(a)–(d) above may also be particularly relevant). Similar considerations could apply if electronic information was inadvertently published online by an entity, or was published online by a third party who had accessed the information from the entity without authorisation, and the information could as a result be accessed by a person with the capability and motive to cause serious harm to affected individuals (such as a person capable of using the information to commit identity theft for financial gain, or in the case of encrypted information, a person capable of converting the information into a form that would be intelligible to an ordinary person as per paragraphs 26WB(3)(c) and (d) above).

53. Paragraph 26WB(3)(g) may be particularly relevant in cases where information compromised in a data breach would not be intelligible to an ordinary person (as per paragraphs 26WB(3)(c) and (d) above, and paragraph 26WB(4) below), but may be intelligible to a person with knowledge or capabilities exceeding those of an ordinary person. An example in relation to electronic information would be a person with access to software or other technology that is not publicly available or commonly used and which could be used to convert the information into a form that would be intelligible to an ordinary person.

54. Paragraph 26WB(3)(h) provides that the nature of the harm that may occur as a result of a data breach is a relevant matter when determining whether a real risk of serious harm exists. The kinds of harm specified in new section 26WF below, and the definition of 'real risk' in new section 26WG below, may be relevant when considering this matter.

55. Paragraph 26WB(3)(i) provides that, if an entity has taken, is taking, or will take steps to mitigate the harm to affected individuals following a data breach:

- the nature of those steps (subparagraph 26WB(3)(i)(i))
- how quickly those steps have been, are being, or will be, taken (subparagraph 26WB(3)(i)(ii)), and
- the extent to which those steps have mitigated, are mitigating, or are likely to mitigate, the harm (subparagraph 26WB(3)(i)(iii)

are relevant when determining whether a real risk of serious harm exists. In some cases prompt, effective action upon discovery of a data breach may prevent a real risk of serious harm to affected individuals from arising or lessen the associated level of risk to affected individuals. Examples of action that may lessen the associated level of risk to affected individuals might include stopping an unauthorised practice, recovering records subject to unauthorised access, unauthorised disclosure or loss, shutting down a system that was subject to unauthorised access or unauthorised disclosure, or remotely erasing the memory of a lost or stolen device. More detailed examples of steps that could reduce the risk of harm associated with a data breach to at least some extent could include:

- A financial institution which becomes aware that customer account details have been compromised in a data breach, and promptly freezes the affected accounts.

- An entity which becomes aware of a breach involving unauthorised access to, or unauthorised disclosure of, passwords for user accounts on an online system, and promptly resets all user passwords.

56. Considerations under subparagraph 26WB(3)(i)(ii) about how quickly steps have been, are being or will be taken to mitigate harm to affected individuals will vary depending on the circumstances. For example, in some situations effectively mitigating a particularly high risk of serious harm may require an entity to take immediate action. In that situation, if the entity fails to act immediately, the harm mitigation may be ineffective.

57. Similarly, considerations under subparagraph 26WB(3)(i)(iii) about the extent to which steps taken have mitigated, are mitigating, or are likely to mitigate the harm will vary depending on the circumstances. If the steps in question have not, are not or are not likely to mitigate a real risk of serious harm following a data breach, the breach may still meet the definition of a 'serious data breach' in new section 26WB unless other considerations apply.

58. Paragraph 26WB(3)(j) provides that any other relevant matter is a relevant matter under paragraph 26WB(3) when determining whether a real risk of serious harm exists to affected individuals following a data breach. The nature of other matters that may be relevant will vary depending on the circumstances of the entity and the data breach. The Commissioner may choose to issue guidance material to assist entities to identify other relevant matters when determining whether a real risk of serious harm exists.

59. New subsection 26WB(4) provides that, for the purposes of applying paragraphs 26WB(3)(c) and (d) above to electronic information, the entity should assume that the 'ordinary person' in question has access to software or other technology that is publicly available (paragraph 26WB(4)(a)) and commonly used (paragraph 26WB(4)(b)). This provision clarifies the scope of the 'ordinary person' test used in paragraphs 26WB(3)(c) and (d) above by introducing the assumption that an ordinary person has access to what are essentially 'ordinary' resources.

60. The terms 'publicly available' and 'commonly used' are intended to cover software or other technology that is available for purchase or for free and is widely used. Software or other technology that is openly available via the internet would be considered 'publicly available', although whether such software or other technology is 'commonly used' would

need to be determined on a case-by-case basis. Examples of software that could be considered publicly available and commonly used could include widely used web browsers, or applications such as Adobe Acrobat Reader, Adobe Photoshop, Microsoft Office, Winzip or equivalent products.

61. As an example of how new subsection 26WB(4) may apply, an entity that inadvertently discloses an unencrypted electronic file containing personal information stored in a commonly used spreadsheet format could assume that the ordinary person referred to in paragraphs 26WB(3)(c) and (d) has access to publicly available, commonly used software capable of reading the information. In this scenario, the information would most likely be 'intelligible' to an ordinary person for the purposes of paragraph 26WB(3)(c) above. On the other hand, if the file was encrypted in such a way that it would not be accessible to an ordinary person with access to publicly available and commonly used software or technology, the likelihood of the information being intelligible to an ordinary person for the purposes of paragraph 26WB(3)(c) would be low.

62. However, new subsection 26WB(4) is not intended to preclude consideration about whether the information is in a form that could only be converted into a form intelligible to an ordinary person via the use of software or other technology that is not publicly available and commonly used. These matters may instead be particularly relevant when determining the likelihood that the information could be converted into a form that is intelligible to an ordinary person under paragraph 26WB(3)(d) above.

63. Similarly, new subsection 26WB(4) does not preclude entities from taking into account the potential use of software or other technology that is not publicly available and commonly used when considering the likelihood that security measures protecting the information could be overcome (paragraph 26WB(3)(f) above), or the persons or kinds of persons who have obtained, or may obtain the information (paragraph 26WB(3)(g) above).

64. The reference to 'software, or other technology' in new subsection 26WB(4) is intended to provide flexibility in the event that an ordinary person could have access to publicly available, commonly used hardware, such as a particular device or kind of device, that could help render the information intelligible (whether in isolation or when used in conjunction with particular software or technology, such as a smartphone on which a particular application is installed). The reference is also intended to provide flexibility in the event that new technologies impact on common methods of accessing and manipulating electronic information. This is consistent with the ALRC's view that, although the Privacy Act's privacy principles should be technology neutral (as the APPs are), the Act should remain 'technology aware' where appropriate.

Overseas recipients

65. New subsection 26WB(5), which is titled 'Overseas recipients', establishes the circumstances under which an APP entity will retain accountability for a 'serious data breach' involving personal information even though that APP entity might not be otherwise responsible for the breach due to the fact that the information has been disclosed to an overseas recipient.

66. New subsection 26WB(5) provides that where:

- an APP entity has disclosed personal information about one or more individuals to an overseas recipient
- APP 8.1 applied to that disclosure, and
- the overseas recipient holds the personal information

then new section 26WB of the Privacy Act applies as if the personal information was held by the APP entity, and the APP entity was required under section 15 of the Privacy Act not to do an act, or engage in a practice, that breaches APP 11.1 in relation to the personal information. This means that the requirements of new subsections 26WB(1) and 26WB(2) apply, and the disclosing APP entity retains accountability under section 16C of the Privacy Act for that personal information, even if the serious data breach occurred offshore.

Bodies or persons with no Australian link

67. New subsection 26WB(6), which is titled 'Bodies or persons with no Australian link', establishes the circumstances under which a credit provider will retain accountability for a 'serious data breach' involving credit eligibility information that was disclosed to a body or person with no Australian link.

68. New subsection 26WB(6) provides that where:

- either:
    - a credit provider has disclosed, under paragraph 21G(3)(b) or (c) of the Privacy Act, credit eligibility information about one or more individuals to a related body corporate, or person, that does not have an Australian link, or
    - a credit provider has disclosed, under subsection 21M(1) of the Privacy Act, credit eligibility information about one or more individuals to a body or person that does not have an Australian link, and
- the related body corporate, body or person holds the credit eligibility information

then new section 26WB of the Privacy Act applies as if the credit eligibility information was held by the credit provider, and the credit provider was required to comply with subsection 21S(1) of the Privacy Act in relation to the credit eligibility information. This means that the requirements of new subsections 26WB(1) and 26WB(2) apply, and the credit provider retains accountability for that credit eligibility information, even where a credit provider discloses credit eligibility information to a recipient that does not have an Australian link. The term 'Australian link' is used to define the entities that are subject to the operation of the Privacy Act, and is used throughout the Act, for example, in section 5B, APP 8 and throughout the credit reporting provisions. This subsection will apply where credit eligibility information has been disclosed by the credit provider to the entities listed in the specified circumstances, and where these entities hold that information.

69. This item also inserts a Note following subsection 26WB(6) and before new section 26WC. The Note provides a cross-reference to section 21NA of the Privacy Act, about disclosures to certain persons and bodies that do not have an Australian link.

Division 3—Notification of serious data breaches

Section 26WC Entity must notify serious data breach

70. This section sets out the circumstances in which an entity must provide notification of a serious data breach and to whom notification must be given. The section also sets out the circumstances in which an entity may be exempted or excepted from an obligation to notify a serious data breach.

71. New subsection 26WC(1) provides that if an entity is aware, or ought reasonably to be aware, that there are reasonable grounds to believe that there has been a serious data breach of the entity (as defined in new section 26WB), the entity must, as soon as practicable after the entity becomes aware, or ought reasonably to have become so aware:

- prepare a statement that complies with new subsection 26WC(3) (paragraph 26WC(1)(a)) (**a paragraph 26WC(1)(a) statement**)

- give a copy of the paragraph 26WC(1)(a) statement to the Commissioner (paragraph 26WC(1)(b))

- take such steps (if any) as are reasonable in the circumstances to notify the contents of the paragraph 26WC(1)(a) statement to each of the individuals to whom the relevant information relates (paragraph 26WC(1)(c)), and

- if it is not practicable for the entity to notify the contents of the paragraph 26WC(1)(a) statement to each of the individuals to whom the information relates:

    - publish a copy of the paragraph 26WC(1)(a) statement on the entity's website (if any) (subparagraph 26WC(1)(d)(i)), and

    - take reasonable steps to publicise the contents of the statement (subparagraph 26WC(1)(d)(ii)).

72. The inclusion of the phrase 'reasonable grounds' in new subsection 26WC(1) is intended to ensure that notification is required both in cases where an entity is aware that a serious data breach has occurred and where the evidence is not definitive but would nonetheless suggest that there are reasonable grounds to believe that a serious data breach has occurred. What constitutes 'reasonable grounds' will vary depending on the circumstances. Where an entity is aware at one particular point in time that there are reasonable grounds to believe that a serious data breach has occurred—for example, where a pattern of complaints suggest a serious data breach may have occurred—but determines after conducting a reasonable assessment within 30 days that there are in fact not such reasonable grounds (for example, because the entity immediately took steps that mitigated the risk of harm), new

subsections 26WC(2) and (14) below together explicitly provide that the notification requirement in new subsection 26WC(1) does not apply, and is taken to have never applied.

73. The 'ought reasonably to be aware' requirement in new subsection 26WC(1) means that entities who fail to become aware that there are reasonable grounds to believe that a serious data breach of the entity has occurred will be in breach of the notification requirement in new section 26WC if the entity ought reasonably to have become so aware in all the circumstances. An example would be an entity that fails to consider whether complaints or other credible forms of evidence suggest that a serious data breach has occurred, or an entity that becomes aware of a data breach but fails to adequately consider whether there may be a real risk of serious harm to affected individuals as a result. In cases such as these, the Commissioner can direct the entity to notify the serious data breach under new section 26WD below.

74. The 'ought reasonably to be aware' requirement in new subsection 26WC(1) would not apply in cases where it is not clear that an entity ought reasonably to be aware of a serious data breach, for example where evidence of the breach or the resulting risk of harm to individuals is obscure or unreasonably difficult to determine. In cases where an entity is unsure whether there are reasonable grounds to believe that a serious data breach has occurred, new subsection 26WC(2) below may also apply, meaning that the entity will have time to consider whether there are reasonable grounds to believe that a serious data breach has occurred before notification will be required.

75. In relation to the requirement in paragraph 26WC(1)(b) to give a copy of the paragraph 26WC(1)(a) statement to the Commissioner, the Commissioner may choose to publish guidance to assist entities to comply with this requirement. For example, the guidance material could ask entities to send a copy of the paragraph 26WC(1)(a) statement to a particular email address, or include details about additional information the Commissioner may ask entities to provide about a serious data breach if the Commissioner considers that the information is required to undertake his or her functions under the Privacy Act.

76. Paragraph 26WC(1)(c) will require entities to take such steps (if any) as are reasonable in the circumstances to notify each individual to whom information involved in a serious data breach relates. The concept of 'taking such steps (if any) as are reasonable in the circumstances' is used elsewhere in the Privacy Act. As noted in the Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, the phrase 'reasonable in the circumstances' is an objective test that ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps in question. The inclusion of the phrase 'if any' means that in some circumstances it may be reasonable for an entity to take no steps: an example in the context of paragraph 26WC(1)(c) might be if the entity does not have contact details for the individuals affected by a serious data breach.

77. This flexibility is necessary given the different types of entities that are to be regulated under the new scheme. For example, for entities with particular functions or engaged in certain activities, it may not be 'reasonable in the circumstances' to notify about a data breach. For example, it may not be reasonable in the circumstances for an entity to

notify particular individuals about a data breach, where that entity has been advised by a law enforcement agency or intelligence agency that notification might prejudice or adversely affect a law enforcement investigation or intelligence-related activity. However, the entity would still be required to comply with paragraph 26WC(1)(b) and provide a copy to the Commissioner unless the entity applied to the Commissioner for an exemption from new subsection 26WC(1) on public interest grounds (see new subsections 26WC(6)–(11) below).

78. The requirement to take such steps (if any) to notify affected individuals will apply even in cases where information about multiple individuals is compromised in a serious data breach, but only some of those individuals are at real risk of serious harm as a result. This recognises that, particularly where a serious data breach involves a large number of individuals, it may require an unreasonable volume of resources for an entity to assess which affected individuals are at real risk of serious harm and which are not. Notification to the entire 'cohort' of affected individuals may actually reduce the cost of compliance for entities, and would also allow each individual to consider whether they need to take any action in response to the serious data breach.

79. An example of how paragraph 26WC(1)(c) could apply would be a serious data breach involving unauthorised access to an entity's customer database which contained the credit card details of some individuals but not others, where the real risk of serious harm arising from the data breach involves potential credit card fraud that could only apply to the former group. Following notification, individuals in the former group could consider cancelling their credit card or alerting their financial institution to the potential risk of fraud, while individuals in the latter group could consider whether they are at real risk of serious harm. If notifying each affected individual under paragraph 26WC(1)(c) is not practicable, the entity could consider whether the alternate notification arrangements in paragraph 26WC(1)(d) below are available.

80. Paragraph 26WC(1)(d) will deal with situations where notifying each affected individual is not practicable. The phrase 'not practicable' is intended to cover situations where the time, effort or cost of notifying each affected individual, when considered in all the circumstances of the entity and the data breach, would render such notification impracticable. In situations where notifying each affected individual is not practicable, publishing a copy of the paragraph 26WC(1)(a) statement on the entity's website (if the entity has a website) is a suitable substitute notification method (subparagraph 26WC(1)(d)(i)), so long as the entity also takes reasonable steps to publicise the contents of the statement (subparagraph 26WC(1)(d)(ii)).

81. The intended purpose of taking reasonable steps to publicise the contents of the paragraph 26WC(1)(a) statement under subparagraph 26WC(1)(d)(ii) is to increase the likelihood that the serious data breach described in the statement comes to the attention of affected individuals. The subparagraph is phrased in technology neutral terms to allow entities to choose the publication channels most likely in the circumstances to be effective in bringing a serious data breach to the attention of affected individuals. Examples that may be reasonable depending on the circumstances include taking out a print or online advertisement in a publication or website the entity considers reasonably likely to reach affected individuals, or publishing an announcement on the entity's social media channels.

82. In some cases (such as a serious data breach that carries a higher risk of serious harm, or that affects a large number of individuals), it might be reasonable to take more than one step to publicise the contents of the paragraph 26WC(1)(a) statement under subparagraph 26WC(1)(d)(ii). For example, if it is reasonable to do so, an entity could take out multiple print or online advertisements (which could include paid advertisements on social media channels), publish posts on multiple social media channels, or use both traditional media and online channels.

83. Possible approaches to publicising the contents of the paragraph 26WC(1)(a) statement as required under subparagraph 26WC(1)(d)(ii) are likely to vary depending on the particular channel or channels chosen to do so. For example, where space and cost allows, the entity may choose to simply republish the entirety of the information required to be included in the paragraph 26WC(1)(a) statement. Another option, if the available space is limited, or the cost of republishing the entire statement would not be reasonable in all the circumstances, would be to summarise the information required to be included in the statement and provide a hyperlink to the copy of the statement published on the entity's website under subparagraph 26WC(1)(d)(i) (bearing in mind that the ability and likelihood of affected individuals being able to access the statement online may determine the appropriateness of relying solely on such an approach). Entities may also choose to adopt both approaches if they are taking multiple reasonable steps under subparagraph 26WC(1)(d)(ii), and the capabilities or requirements of the chosen channels vary.

84. Where an entity considers that compliance with paragraph 26WC(1)(d) would be practicable but nonetheless contrary to the public interest, the entity may apply to the Commissioner for an exemption from the notification requirement (see new subsections 26WC(6)–(11) below).

85. New subsection 26WC(2) provides that the phrase 'as soon as practicable' in new subsection 26WC(1) includes time taken by the entity to carry out a reasonable assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to a serious data breach of the entity, so as long that assessment is carried out within 30 days. This subsection is intended to operate in cases where:

- an entity is not certain, but ought reasonably to be aware, that there are reasonable grounds to believe there has been a serious data breach of the entity, and a reasonable assessment of relevant circumstances would allow the entity to determine that subsection 26WC(1) applies, or

- an entity is aware that there are reasonable grounds to believe that a serious data breach has occurred, but nonetheless believes that a reasonable assessment is likely to reveal that a serious data breach has in fact not occurred.

86. The intention of the assessment process mentioned in new subsection 26WC(2) is twofold:

- to make clear that entities will not breach the 'as soon as practicable' timeframe in section 26WC(1) simply because of the time undertaken to reasonably assess whether notification under new section 26WC(1) is required, and

- to discourage entities from acting out of an abundance of caution to notify a data breach incident where, following a reasonable assessment, the entity would have determined that there are not actually reasonable grounds to believe that a serious data breach has occurred.

87. The assessment process is therefore intended to provide certainty and reduce the cost of compliance for entities and reduce the risk of individuals experiencing 'notification fatigue' due to receiving large numbers of notifications for non-serious breaches.

88. The 30 day timeframe is intended to provide entities with certainty about how long they have to assess the relevant circumstances, without unduly delaying notification to affected individuals if the assessment determines that notification is required. Entities could also choose to complete an assessment in a shorter time period of possible, for example where an entity only requires a matter of hours or a few days to determine that notification is required. Entities may also choose to fast track an assessment if a potential serious data breach would have a particularly high impact on affected individuals.

89. The nature of an assessment under new subsection 26WC(2) will vary depending on the circumstances of the serious data breach or potential serious data breach. For example, in some cases the entity may need to assess whether unauthorised access to or unauthorised disclosure of information has occurred, or (in the case of loss of information) is likely to occur. On the other hand, if the entity has reasonable grounds to believe that unauthorised access or unauthorised disclosure has occurred or is likely to have occurred, the assessment may focus solely on the potential harm to individuals (in which case the matters listed in new subsection 26WB(3) above could assist entities in undertaking the assessment).

90. The reference to a 'reasonable' assessment in new subsection 26WC(2) reflects an intention that an assessment should be limited to matters that are reasonably likely to be relevant in the circumstances. An assessment which considers a range of matters which could not reasonably be considered relevant in the circumstances would not fall within the scope of this section.

91. The action required after undertaking a reasonable assessment as per new subsection 26WC(2) will depend both on the results of the assessment and whether the entity, before undertaking the assessment, was aware that there were reasonable grounds to believe that a serious data breach has occurred. For example:

- if the entity was not aware of such reasonable grounds before undertaking an assessment, and the assessment determines that there are no such reasonable grounds, notification under new subsection 26WC(1) is not (and was never) required

- if an entity was aware of such reasonable grounds before undertaking an assessment, but the assessment determines that there are in fact no such reasonable grounds, new

subsection 26WC(1) is taken to not apply, and to have never applied (see new subsection 26WC(14) below)

- regardless of whether or not an entity was aware of such reasonable grounds before undertaking an assessment, if the assessment determines or confirms that there are in fact such reasonable grounds, the entity would be required to undertake notification under new subsection 26WC(1) (though the entity would not be deemed to have contravened 'as soon as practicable' timeframe in that subsection solely because of the time taken to carry out the assessment).

92. New subsection 26WC(3) sets out the contents of the paragraph 26WC(1)(a) statement that an entity must prepare to give notice of a serious data breach. These are based on the matters in the current OAIC *Data Breach Notification: A guide to handling personal information security breaches*. The statement must include:

- the identity and contact details of the entity (paragraph 26WC(3)(a))
- a description of the serious data breach that the entity has reasonable grounds to believe has happened (paragraph 26WC(3)(b))
- the kind or kinds of information concerned (paragraph 26WC(3)(c)), and
- recommendations about the steps that individuals should take in response to the serious data breach that the entity has reasonable grounds to believe has happened (paragraph 26WC(3)(d)).

93. The recommendations that must be included in the paragraph 26WC(1)(a) statement under paragraph 26WC(3)(d) are intended to provide individuals whose information has been compromised in a serious data breach with advice about steps they should take to mitigate the harm that may arise to them as a result. Examples could include recommending that individuals request a copy of their credit report if a serious data breach might result in credit fraud.

94. The list of matters in subsection 26WC(3) that the paragraph 26WC(1)(a) statement must include is not an exhaustive list. Entities would have the discretion to include other information, for example, an apology to affected individuals. Guidance material from the Commissioner may identify other kinds of information that entities may wish to consider including in a paragraph 26WC(1)(a) statement in addition to the information that must be included under paragraph 26WC(3).

Method of providing the statement to an individual

95. Without limiting paragraph 26WC(1)(c), new subsection 26WC(4), which is titled 'Method of providing the statement to an individual', provides that where an entity normally communicates with an individual using a particular method, any notifications provided to the individual under paragraph 26WC(1)(c) may use that method. This is intended to reduce the cost of compliance for entities but also to ensure that individuals receive notifications through communication channels that they expect relevant entities to use. Where there is no normal

mode of communication with the particular individual the entity must take reasonable steps to communicate with him or her. Reasonable steps could include contact by email, telephone or post.

Exception—enforcement related activities

96. New subsection 26WC(5), which is titled 'Exception—enforcement related activities', provides that paragraphs 26WC(1)(c), 26WC(1)(d) and 26WC(3)(d) do not apply if the relevant entity is a law enforcement body that believes on reasonable grounds that compliance with those paragraphs would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, the enforcement body.

97. 'Enforcement body' and 'enforcement related activities' are defined in subsection 6(1) of the Privacy Act. The effect of this provision is that a law enforcement body is not required to notify affected individuals of the contents of the paragraph 26WC(1)(a) statement, either individually or in compliance with paragraph 26WC(1)(d) above. However, with the exception of paragraph 26WB(3)(d), the entity must still comply with paragraphs 26WC(1)(a) (i.e., the entity must prepare a statement that complies with paragraphs 26WC(3)(a), (b) and (c)) and 26WC(1)(b) (i.e. the entity must give a copy of that statement to the Commissioner).

98. The rationale for not requiring an entity in these circumstances to prepare a statement that complies with paragraph 26WC(3)(d), which deals with recommendations about steps individuals should take in response to a serious data breach, is that providing these recommendations to the Commissioner will serve no utility if affected individuals are not being notified of the serious data breach.

99. This exception is intended to ensure that the legitimate activities of enforcement bodies are not disrupted or affected by the notification requirement. However, it does not extend to serious data breaches that are not related to enforcement activities such as the inadvertent disclosure of personal information unrelated to investigations or intelligence gathering. It also ensures that notification to the Commissioner is still required, so that the Commissioner can advise and assist enforcement bodies in responding to data breaches, and can continue to collect important information about data breaches to assist in combating or addressing them into the future.

Exception—Commissioner's notice

100. New subsection 26WC(6), which is titled 'Exception—Commissioner's notice', provides that the Commissioner may, by written notice given to an entity, exempt that entity from the requirement to notify contained in new subsection 26WC(1), in such circumstances that are contained in that written notice (**a subsection 26WC(6) notice**).

101. New subsection 26WC(7) provides that a subsection 26WC(6) notice can only be given when the Commissioner is satisfied that it is in the public interest to do so. It is expected that the Commissioner will develop guidance in consultation with all relevant stakeholders on what factors will need to be taken into account in determining whether issuing a notice will be in the public interest.

102. In that respect, the ALRC commented that such a provision could cover situations, for example, where there is a law enforcement investigation being undertaken into a data breach and notification would impede that investigation, or where the information concerned matters of national security. This provision is intended to cover cases of that nature (where these activities, or the information concerned, are not already exempt from the scheme), particularly where a private sector organisation suffers the data breach and is responsible for reporting. In those situations, it is expected that a private sector organisation or Commonwealth agency would seek or have otherwise already received advice from an enforcement body or intelligence agency before applying to the Commissioner for a notice.

103. New subsection 26WC(8) provides that the Commissioner may issue a subsection 26WC(6) notice either on the Commissioner's own initiative or on application made by the entity. A decision by the Commissioner to refuse to issue a subsection 26WC(6) notice on application by the entity will be reviewable by the Administrative Appeals Tribunal (see Item 4 below).

104. New subsection 26WC(9) provides that an entity is only entitled to apply to the Commissioner under paragraph 26WC(8)(b) if the entity believes on reasonable grounds that a serious data breach has occurred. This provision is intended to discourage entities from making an application if they do not have reasonable grounds to believe a serious data breach has occurred, and should in that way allow entities to avoid any costs which might have been incurred in unnecessarily lodging an application. Where an entity is uncertain as to whether there are reasonable grounds to believe a serious data breach has occurred, new subsection 26WC(2) above makes clear that the entity has 30 days to reasonably assess whether there are such reasonable grounds before the entity is required to notify the Commissioner and affected individuals. If, after undertaking such an assessment, the entity forms the view that there are reasonable grounds to believe that a serious data breach has occurred, the entity would be entitled to apply to the Commissioner under paragraph 26WC(8)(b). Entities applying to the Commissioner under paragraph 26WC(8)(b) would be required to do so as soon as practicable after the entity became aware, or ought reasonably to have become aware, of the serious data breach, consistent with the notification timeframes in new subsection 26WC(1) above.

105. New subsection 26WC(10) provides that, where the Commissioner refuses an application made by an entity under paragraph 26WC(8)(b) for a subsection 26WC(6) notice, the Commissioner must give written notice of the refusal.

106. New subsection 26WC(11) provides that, if an entity applies to the Commissioner for an exemption under paragraph 26WC(8)(b), after having reasonable grounds to believe that a serious data breach has occurred, the requirement to notify contained in new subsection 26WC(1) will not apply until the Commissioner makes a decision in response to the application. This provision is intended to suspend an entity's obligation to notify while waiting for the Commissioner to make a decision on the public interest application. The provision is intended to make clear that the entity will not be in breach of notification obligations solely because of the time required for the Commissioner to consider the entity's application for a subsection 26WC(6) notice. The provision is not intended to cure a breach

of new subsection 26WC(1) that has already occurred before the entity applies to the Commissioner for a subsection 26WC(6) notice.

Exception—inconsistency with secrecy provisions

107. New subsection 26WC(12), which is titled 'Exception—inconsistency with secrecy provisions', provides that, if compliance by an entity with paragraph 26WC(1)(b), (c) or (d) of the Privacy Act would, to any extent, be inconsistent with a provision of a law of the Commonwealth (other than a provision of the Privacy Act) that prohibits or regulates the use or disclosure of information, the requirement to notify contained in new subsection 26WC(1) does not apply to the entity to the extent of the inconsistency.

108. The effect of this provision is to make it clear that the secrecy provisions contained in other Commonwealth legislation prevail over the requirement to notify in new subsection 26WC(1) of the Privacy Act. For example, new subsection 26WC(12) will ensure that there is no conflict between the Privacy Act and the provisions of other acts which prohibit disclosure of official information or secrets by Commonwealth officers (such as sections 70 and 79 of the *Crimes Act 1914* (Cth)).

Exception—My Health Records Act 2012

109. New subsection 26WC(13), which is titled 'Exception—My Health Records Act 2012', provides that new subsection 26WC(1) does not apply to a serious data breach if the breach has been, or is required to be, notified under section 75 of the *My Health Records Act 2012* (**My Health Records Act**). This provision has the effect of preventing the imposition of a double notification requirement on entities that are required to comply with section 75 of the My Health Records Act in relation to the same data breach.

Exception—no serious data breach

110. New subsection 26WC(14), which is titled 'Exception—no serious data breach', provides that new subsection 26WC(1) does not apply, and is taken to have never applied, if:

- at a particular time, an entity was aware, or ought reasonably to have been aware, of reasonable grounds to believe that there had been a serious data breach of the entity
- the entity subsequently carries out a reasonable assessment (as per new subsection 26WC(2) above) of whether there are in fact such reasonable grounds
- the assessment was carried out within 30 days after the entity became aware, or ought reasonably to have become aware, as the case may be, and
- after carrying out the assessment, the entity determines that it does not in fact have such reasonable grounds.

111. This provision is intended to operate in parallel with new subsection 26WC(2) above to help reduce the cost of compliance for entities and the risk of 'notification fatigue' for individuals arising from notification of data breaches that do not carry a real risk of serious

harm. Together, new subsections 26WC(2) and (14) will ensure that, if an entity was aware, or ought reasonably to have been aware, at a particular point in time that there were reasonable grounds to believe that a serious data breach had occurred, but determines after a reasonable assessment of the circumstances (carried out within 30 days) that there are in fact no such reasonable grounds, the entity is not taken to have contravened new subsection 26WC(1), or to have any ongoing obligations under that subsection.

Section 26WD Commissioner may direct entity to notify serious data breach

112. This section provides the Commissioner with the power to direct an entity to provide notification of a serious data breach. It is envisaged that this provision may be enlivened in circumstances such as where a serious data breach comes to the attention of the Commissioner but has not come to the attention of an entity.

113. New subsection 26WD(1) provides that if the Commissioner believes on reasonable grounds that there has been a serious data breach of the entity, the Commissioner may, by written notice given to the entity, direct the entity to:

- prepare a statement that complies with new subsection 26WD(2) (paragraph 26WD(1)(a)) (**a paragraph 26WD(1)(a) statement**)
- give a copy of the paragraph 26WD(1)(a) statement to the Commissioner (paragraph 26WD(1)(b))
- take such steps (if any) as are reasonable in the circumstances to notify the contents of the paragraph 26WD(1)(a) statement to each of the individuals to whom the relevant information relates (paragraph 26WD(1)(c)), and
- if it is not practicable for the entity to notify the contents of the paragraph 26WD(1)(a) statement to each of the individuals:
    - publish a copy of the paragraph 26WD(1)(a) statement on the entity's website (if any) (subparagraph 26WD(1)(d)(i)), and
    - take reasonable steps to publicise the contents of the statement (subparagraph 26WD(1)(d)(ii)).

114. Before issuing a direction under new subsection 26WD(1) **(a subsection 26WD(1) direction)**, the Commissioner must have 'reasonable grounds' to believe that a serious data breach of the entity has occurred. For example, a complaint or series of similar complaints from individuals about an entity might lead the Commissioner to form the belief on reasonable grounds that the entity has experienced a serious data breach.

115. New subsection 26WD(2) sets out the contents of the paragraph 26WD(1)(a) statement that an entity must prepare to give notice of a serious data breach. These are based on the matters that must be included when an entity has an obligation to notify a serious data breach under new subsection 26WC(1) (see new subsection 26WC(3)). The statement must include:

- the identity and contact details of the entity (paragraph 26WD(2)(a))

- a description of the serious data breach that the Commissioner believes has happened (paragraph 26WD(2)(b))

- the kinds of information concerned (paragraph 26WD(2)(c)), and

- recommendations about the steps that individuals should take in response to the data breach that the Commissioner believes has happened (paragraph 26WD(2)(d)).

116. New subsection 26WD(3) provides that the Commissioner, in issuing a subsection 26WD(1) direction, may also require that the paragraph 26WD(1)(a) statement set out specified information that relates to the serious data breach that the Commissioner believes has happened. This provision is intended to operate in cases where the Commissioner considers that it is reasonable and appropriate for individuals to be provided with additional information about the data breach, for example, where the impact of a serious data breach on individuals is particularly high, such as if individuals are at increased risk due to the time that has elapsed since the serious data breach occurred. The specified information that relates to a serious data breach is intended to be information that the Commissioner considers would assist individuals to take appropriate action in response to the serious data breach. Examples could include:

- information about the real risk of serious harm to individuals that the Commissioner considers exists as a result of the serious data breach

- recommendations about steps the Commissioner considers individuals should take in response to the serious data breach

- information about complaint mechanisms available under the Privacy Act to individuals affected by the serious data breach, or

- other specified information relating to the serious data breach that the Commissioner considers reasonable and appropriate in the circumstances to include in the paragraph 26WD(1) statement.

117. The Commissioner would not be required to specify additional information that must be set out in a paragraph 26WD(1)(a) statement under subsection 26WD(3). A decision by the Commissioner to require the inclusion of specified information relating to the serious data breach in the paragraph 26WD(1)(a) statement would be reviewable by the Administrative Appeals Tribunal as part of the general ability to seek review of a direction to notify a serious data breach (see Item 4 below).

Method of providing the statement to an individual

118. Without limiting paragraph 26WD(1)(c), new subsection 26WD(4), which is titled 'Method of providing the statement to an individual', provides that where an entity normally communicates with an individual using a particular method, any notifications provided to the individual under paragraph 26WD(1)(c) may use that method. This is intended to reduce the

cost of compliance for entities but also to ensure that individuals receive notifications through communication channels that they expect relevant entities to use. Where there is no normal mode of communication with the particular individual, the entity must take reasonable steps to communicate with him or her. Reasonable steps could include contact by email, telephone or post.

Compliance with direction

119. New subsection 26WD(5), which is titled 'Compliance with direction', provides that an entity must comply with a subsection 26WD(1) direction as soon as practicable after the direction is given.

Exception—enforcement related activities

120. New subsection 26WD(6), which is titled 'Exception—enforcement related activities', provides that the Commissioner must not give a subsection 26WD(1) direction to an entity that is a law enforcement body if the chief executive officer of that law enforcement body has given the Commissioner a certificate stating that the enforcement body believes on reasonable grounds that compliance with the direction would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body.

121. 'Enforcement body' and 'enforcement related activities' are defined in subsection 6(1) of the Privacy Act. This exception is intended to ensure that the legitimate activities of enforcement bodies are not disrupted or affected by the notification requirement. However, it does not extend to serious data breaches that are not related to enforcement activities such as the inadvertent disclosure of personal information unrelated to investigations or intelligence gathering. The requirement that the chief executive of the enforcement body provide the Commissioner with a certificate will ensure that the Commissioner can be assured that the enforcement body has formed the relevant belief on reasonable grounds.

122. It is expected that, where the Commissioner intends to issue a direction under new subsection 26WD(1) to an enforcement body, the Commissioner would wherever possible consult with the enforcement body beforehand, so that the enforcement body has the opportunity to consider whether or not to issue a certificate in accordance with new subsection 26WD(6).

Exception—inconsistency with secrecy provisions

123. New subsection 26WD(7), which is titled 'Exception—inconsistency with secrecy provisions', provides that, if compliance by an entity with a subsection 26WD(1) direction as is covered by paragraph 26WD(1)(b), (c) or (d) would, to any extent, be inconsistent with a provision of a law of the Commonwealth (other than a provision of this Act) that prohibits or regulates the use or disclosure of information, paragraph 26WD(1)(b), (c) or (d), as the case may be, does not apply to the entity to the extent of the inconsistency.

124. The effect of this provision is to make it clear that the secrecy provisions contained in other Commonwealth legislation prevail over the requirement to comply with a

subsection 26WD(1) direction. For example, new subsection 26WD(7) will ensure that there is no conflict between the Privacy Act and the provisions of other acts which prohibit disclosure of official information or secrets by Commonwealth officers (such as sections 70 and 79 of the *Crimes Act 1914* (Cth)).

Exception—My Health Records Act 2012

125. New subsection 26WD(8), which is titled 'Exception—My Health Records Act 2012', provides that the Commissioner must not give a subsection 26WD(1) direction in relation to a serious data breach if the breach has been, or is required to be, notified under section 75 of the My Health Records Act. This provision has the effect of preventing the imposition of a double notification requirement on entities that are required to comply with section 75 of the My Health Records Act in relation to the same data breach.

Division 4—General

Section 26WE Entity

126. Existing subsection 6(1) of the Privacy Act defines 'entity' to include an agency, an organisation or a small business operator (all of which are also defined in subsection 6(1)). Section 26WE provides that, for the purposes of the new Part IIIC—Notification of serious data breaches, 'entity' also includes a person who is a file number recipient. This will ensure that file number recipients which fall under the definition of 'serious data breach' in new section 26WB above but are not an agency, an organisation or a small business operator will nonetheless still be subject to the notification requirement.

Section 26WF Harm

127. Section 26WF provides that, for the purposes of the new Part IIIC—Notification of serious data breaches, the word 'harm' includes physical harm, psychological harm, emotional harm, harm to reputation, economic harm, and financial harm. This is a non-exhaustive list and is in addition to the ordinary meaning of the word 'harm'. The section is included to provide clarity. The Commissioner may issue practical guidance about identifying forms of 'harm' for the purposes of section 26WF.

Section 26WG Real risk

128. Section 26WG provides that, for the purposes of the new Part IIIC—Notification of serious data breaches, the term 'real risk' means a risk that is not a remote risk.

129. This is an important threshold that is intended to exclude risks that are minor in nature. It would not be appropriate for minor breaches to be notified because of the administrative burden that may place on entities, the risk of notification fatigue on the part of individuals, and the lack of utility where notification does not facilitate mitigation or consideration of whether mitigation is necessary. As is the case in the current OAIC *Data Breach Notification: A guide to handling personal information security breaches*, it is expected that further practical guidance around the concept of a 'real risk of serious harm' will be included in revised OAIC guidance that complements these new reforms.

Item 4 After paragraph 96(1)(b)

130. Item 4 of Schedule 1 inserts new paragraphs 96(1)(ba) and 96(1)(bb) into subsection 96(1) of the Privacy Act, after existing paragraph 96(1)(b). The effect of this insertion is that new paragraphs 96(1)(ba) and 96(1)(bb) respectively provide that a decision by the Commissioner:

- under new section 26WC(10) above to refuse to give a subsection 26WC(6) notice on application by an entity that the entity is exempt from an obligation to notify a serious data breach, and

- under new section 26WD above to give a subsection 26WD(1) direction to an entity to notify a serious data breach

will be subject to review by the Administrative Appeals Tribunal.

Item 5 Application of amendments—serious data breaches

131. Item 5 of Schedule 1 provides that the new Part IIIC—Notification of serious data breaches to be inserted by this Bill applies to an access, disclosure, or loss that occurs after the commencement of Item 5. That is, none of the provisions in the Bill will operate retrospectively. Serious data breaches that occur after the commencement date will be subject to the requirements of the new Part IIIC.