2016

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) BILL 2016

EXPLANATORY MEMORANDUM

(Circulated by authority of the

Attorney-General, Senator the Hon George Brandis QC)

PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) BILL 2016

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. The Government subsequently released exposure draft legislation for public comment between 3 December 2015 and 4 March 2016. Forty-seven public submissions were received on the exposure draft, with submissions generally supporting the legislation or supporting it subject to technical changes. The Attorney-General's Department also undertook targeted consultation with industry and civil society stakeholders about the exposure draft, resulting in a range of feedback and suggestions that were considered when finalising a Bill to present before Parliament.

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 an eligible 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 similar 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 (**the affected 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 an eligible data breach where a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals as a result of the unauthorised access or unauthorised disclosure (assuming, in the case of loss of information, that the access or disclosure occurred). 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)**. An eligible data breach is 'notifiable' (as per the Bill's title) when no exceptions to notification apply.

8. The 'reasonable person' and 'likely risk' elements of the notification standard do not expressly reflect the ALRC's recommended 'real risk of serious harm' standard, which is also used in the OAIC voluntary notification guidelines. These elements, however, respond to significant stakeholder concerns about the practicability of determining what degree of probability and what kind of harm would be captured in the phrase 'real risk of serious harm'. The 'reasonable person' and 'likely risk' elements of the notification standard, by using commonly-understood legal standards of objectivity and probability, are intended to provide greater certainty for regulated entities while maintaining consistency with the core element of the ALRC recommendation.

9. Serious harm, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach. Though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not itself be sufficient to require notification unless a reasonable person in the entity's position would consider that the likely consequences for those individuals would constitute a form of serious harm.

10. It is expected that a likely risk of serious financial, economic or physical harm would be the most common likely forms of serious harm that may give rise to notification. Nonetheless, a reasonable person may conclude in some cases that a likely risk of serious psychological or emotional harm, serious harm to reputation or other serious harms arising from an unauthorised access, unauthorised disclosure or loss of personal information may

exist. For example, this may be the case where an eligible data breach involves health information or other 'sensitive information' (in the sense of the definition of that term in existing subsection 6(1) of the Privacy Act or otherwise).

11. To give rise to an eligible data breach, however, the reasonable person would also need to be satisfied that the risk of serious harm occurring is likely, that is, more probable than not. In deciding whether this is the case, entities are required to have regard to a list of 'relevant matters' included in the Bill. 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.

12. If more than one entity jointly and simultaneously holds the same particular record of personal information, an eligible data breach of one entity may also be an eligible data breach of each of the other entities. This situation could potentially arise in cases involving outsourcing, joint ventures or shared services arrangements. For example, if one entity stores personal information in an online platform provided by another entity, and both entities 'hold' the information (as per the definition in existing subsection 6(1) of the Privacy Act), an eligible data breach involving the information could potentially be an eligible data breach of both entities.

13. In these circumstances the Bill provides that, where one of the entities concerned complies with its obligations under the new Part IIIC in relation to the eligible data breach, each of the entities is taken to have complied with their obligations. The various exceptions, including the Commissioner's ability to grant exemptions, also deal with these circumstances (so that an exception applying to one entity will typically apply to each of the entities). The Bill does not, however, specify which entity must comply with the obligations under Part IIIC in these circumstances. This will be a matter for the relevant entities to determine themselves.

14. If an entity suspects that an eligible data breach has occurred, they must undertake an assessment into the relevant circumstances. In the event of an eligible data breach, an entity is required to notify the Commissioner and affected individuals as soon as practicable after the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach (unless an exception applies). 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.

15. 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 an eligible 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.

16. In providing the information described above to affected individuals, the entity also has discretion to notify either each affected individual or, if not all affected individuals are deemed to be 'at risk' from an eligible data breach, only those affected individuals who are deemed to be at risk. This discretion is intended to provide flexibility to respond to different kinds of eligible data breaches. For example, in some cases it may be impracticable for an entity to consider the circumstances of each affected individual to determine which individuals are at risk from an eligible data breach and which are not. In these circumstances notifying the entire cohort of affected individuals may be appropriate. In other cases it may be practicable for an entity to determine with a high degree of confidence that only some individuals from a broader group of affected individuals are at risk, meaning that notification to the broader group may not be necessary from a harm mitigation perspective.

17. There may be circumstances in which it is impracticable to provide a notification to affected individuals, either collectively or only to those at risk. 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.

18. 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.

19. 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. If compliance would be inconsistent with another law of that kind which is prescribed in regulations under the Privacy Act, an entity will be exempt from the notification requirement. Finally, to avoid creating a double notification requirement, an unauthorised access, unauthorised disclosure or loss of personal information cannot give rise to an eligible data breach if that access, disclosure or loss has been, or is required to be, notified under the mandatory data breach notification requirement in section 75 of the *My Health Records Act 2012* (**the My Health Records Act**).

20. Another exception applies in various circumstances where entities have taken remedial action following an eligible data breach or potential eligible data breach. Specifically, this exception applies where a reasonable person would conclude that, as a

result of the remedial action, the unauthorised access or unauthorised disclosure of personal information (including an unauthorised access or unauthorised disclosure following loss of the information) is not likely to result in serious harm to the affected individuals. The exception also applies where remedial action has prevented a loss of information from leading to an unauthorised access or disclosure. If remedial action following an access or disclosure would lead a reasonable person to conclude that only particular individuals within a broader group are not likely to be at risk of serious harm following the remedial action, the entity is not required to notify those particular individuals (but would still be required to notify the remainder of the individuals).

21. In addition, the Commissioner may exempt an entity from providing notification of an eligible data breach where the Commissioner is satisfied that it is reasonable in the circumstances to do so, having had regard to several matters prescribed in the Bill. The Commissioner may issue an exemption on application from an entity or on the Commissioner's own initiative. The exemption may absolve an entity from complying with the notification requirement altogether or for a period of time that the Commissioner considers reasonable in the circumstances.

22. In deciding whether to grant an exemption, the Commissioner must have regard to any relevant advice about the reasonableness of doing so from a law enforcement body or the Australian Signals Directorate (**ASD**). For example, a law enforcement body may advise the Commissioner that an entity should be granted an exemption for a period of time to avoid compromising an investigation into an eligible data breach, or ASD may advise that notifying an eligible data breach would be likely to lead to further eligible data breaches (for example, if vulnerabilities in an entity's IT security systems became publicly known before they could be rectified).

23. This advice function for ASD reflects ASD's cyber-security expertise and role in providing advice and assistance on information and communications security (including through the Australian Cyber Security Centre).

24. An enforcement body or ASD could approach the Commissioner with relevant advice, the Commissioner could seek relevant advice from them or an entity applying for an exemption could potentially provide a copy of such advice with appropriate bona fides. Regardless, the decision about whether granting an exemption would be reasonable in the circumstances would remain with the Commissioner. The requirement to have regard to advice from these entities would also not prevent the Commissioner from considering other advice when deciding whether to grant an exemption.

25. In circumstances where the Commissioner believes that an eligible data breach has occurred and no notification has been given by the entity that suffered the breach, the Commissioner may give a written direction to the entity requiring it to provide notification of the data breach. Before giving a direction, the Commissioner must invite the entity concerned to make a submission to the Commissioner about the direction, and consider any response from the entity. The Commissioner has discretion to decide on the manner in which the invitation is made and the time the entity has to respond, given that in some cases a long period of time may not be appropriate. As with the exemption process, the Commissioner

must also consider any relevant advice from a law enforcement body or ASD, and has discretion to also consider other advice.

26. Where a direction is given, 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 eligible data breach that the Commissioner considers appropriate in the circumstances. If the eligible data breach in question is an eligible data breach of more than one entity, the Commissioner can also require the entity receiving the direction to include details of each entity concerned.

27. Similarly, the requirements as to communicating with individuals will be the same as though the entity had initiated notification itself. 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. A secrecy provision exception equivalent to that described above will also apply.

28. 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.

29. 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.

30. A decision by the Commissioner to refuse to grant an exemption in response to an application from an entity, to grant an exemption for a lesser period of time than an entity requested, or to give a direction that an entity provide notification of an eligible data breach will be reviewable by the Administrative Appeals Tribunal.

31. 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

32. This Bill has no significant impact on Commonwealth expenditure or revenue.

REGULATION IMPACT STATEMENT

Background

Australian Law Reform Commission Report on Privacy

33. In May 2008, the Australian Law Reform Commission (**ALRC**) concluded a 28 month inquiry into the effectiveness of the *Privacy Act 1988* (**Privacy Act**) and related laws as a framework for the protection of privacy in Australia[1]. The ALRC's report, *For Your Information: Australian Privacy Law and Practice* (**ALRC report**), made 295 recommendations for reform in a range of areas, including creating unified privacy principles, updating the credit reporting system, and strengthening the powers of the Privacy Commissioner. The Government responded to the majority of these recommendations with the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which introduced major privacy reforms and commenced in March 2014.

34. One of the ALRC's other recommendations was that a mandatory data breach notification scheme be introduced (rec 51-1). Submissions to the ALRC's inquiry indicated strong support for the introduction of a mandatory notification requirement, although some key private sector organisations in the banking and telecommunications industries were not supportive[2].

35. The ALRC noted developments in international jurisdictions where legislative reform has been implemented. In particular, the ALRC considered that the United States, where at the time mandatory data breach notification was required in more than 30 states, was at the 'forefront in the development of such laws'[3].

36. After considering submissions and consultations, the ALRC recommended that a data breach notification requirement be introduced in the Privacy Act. The ALRC considered that the test should set a higher threshold for notification than is provided in most other jurisdictions (i.e. a test based on a real risk of serious harm to an affected individual following a data breach, rather than a test that is satisfied whenever a data breach occurs). Amongst other things, the ALRC believed that a higher threshold for notification should also reduce the compliance burden on agencies and organisations.

37. The ALRC also believed that it would be appropriate to allow for a civil penalty to be imposed where an agency or organisation has failed to notify the national privacy regulator (currently the Office of the Australian Information Commissioner (**OAIC**)) of a data breach. The rationale behind this recommendation was that it would provide a strong incentive for agencies and organisations to disclose data breaches where required, and encourage these

[1] See at: http://www.alrc.gov.au/publications/report-108.

[2] ALRC Report, paragraphs 51.52 – 51.56.

[3] ALRC Report, paragraphs 51.3 and 51.14.

entities to consult with the OAIC where a data breach has occurred to ensure they are in full compliance with notification requirements.

Government response to the ALRC Report

38. On 14 October 2009, the Government released a First Stage Response to the ALRC report, which addressed 197 of the Commission's 295 recommendations. Recommendation 51–1 was not part of the 197 recommendations and was identified along with a number of other recommendations as requiring consultation and consideration.

International trends since the ALRC Report

39. Since the ALRC Report, the trend in international jurisdictions has been towards the development and implementation of legislative requirements for notification of data breaches. In the United States, 47 states, the District of Columbia and three territories have implemented mandatory data breach notification[4]. In January 2015, U.S. President Barack Obama proposed a national data breach notification standard in the draft Personal Data Notification & Protection Act. The proposed scheme would require notification if there is any reasonable risk of harm or fraud to individuals following a data breach.

40. Elsewhere, the European Union has introduced regulations that mandate data breach notification. In May 2014, New Zealand announced plans to introduce a two-tier mandatory data breach notification scheme. On 16 June 2015, Canada passed legislation to introduce a national mandatory data breach notification scheme.

Voluntary data breach notification scheme

41. In 2008 the then Office of the Privacy Commissioner (**OPC**) released *Data breach notification — A guide to handling personal information security breaches* (**Data Breach Guide**) in response to requests for advice from agencies and organisations about data breaches, and in recognition of the global trends relating to data breach notification[5]. The Data Breach Guide encouraged entities to voluntarily notify the Privacy Commissioner of data breaches that satisfied the ALRC's recommended 'real risk of serious harm' test, and provided guidance about how to identify and contain a data breach.

42. The OAIC, which replaced the OPC as the national privacy regulator in November 2010, revised the Data Breach Guide in 2011 and 2014 to reflect changing attitudes and approaches to data breach management, and amendments to the Privacy Act. The OAIC also released a companion *Guide to Developing a Data Breach Response Plan in April 2016*[6], following a public consultation process.

[4] *Data Security and Breach Notification Legislation: Selected Legal Issues*, Congressional Research Service, December 28, 2015, p 3.

[5] See the current version of the Data Breach Guide at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

[6] See at: https://oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-a-data-breach-response-plan.

43. The table below captures the number of voluntary data breach notifications made to the OPC/OAIC since 2009-10, when figures about the number of voluntary notifications were first reported separately from the total number of Privacy Commissioner investigations conducted. The number of notifications in 2014-15 was nearly 250% higher than in 2009-10, possibly reflecting increased awareness of privacy obligations among entities following the passage of the *Privacy Amendment (Enhancing Privacy Protection) Act* in November 2012, and the extensive amendments to the Privacy Act that occurred upon its commencement in March 2014.

Table 1: Voluntary data breaches notifications, 2009-10 to 2015-16

Year	**Voluntary data breaches to the privacy regulator**
2009-10	44
2010-11	56
2011-12	46
2012-13	61
2013-14	69
2014-15	110
2015-16	107

Consultation in 2012 and 2013

44. On 19 October 2012, the Government released a Discussion Paper for consultation (**2012 consultation**) seeking public comments on whether Australia's privacy laws should include a mandatory data breach notification requirement and, if so, the possible elements of such a requirement. The 2012 consultation and the responses to it are outlined and analysed in more detail below.

Further 2013 targeted consultation

45. In April 2013, the Government undertook confidential targeted consultation (**2013 targeted consultation**) on a more detailed legislative model. This consultation process invited comments on the legislative model that would form the basis of the Privacy Amendment (Privacy Alerts) Bill 2013 (**Privacy Alerts Bill**). The consultation sought particular views on the possible costs to business.

Privacy Alerts Bill

46. On 29 May 2013, the then Government introduced the Privacy Alerts Bill into the House of Representatives. If passed, the Privacy Alerts Bill would have introduced the

requirement to notify the OAIC and affected individuals where there has been a data breach which gives rise to a 'real risk of serious harm' to an affected individual.

47. The Privacy Alerts Bill was intended to implement ALRC recommendation 51-1 and strengthen the existing voluntary data breach notification framework in order to counter underreporting of data breaches and to help prevent or reduce the effects of serious crimes like identity theft. The Privacy Alerts Bill was based on the general requirements of the Privacy Act's Australian Privacy Principle (**APP**) 11 in the Privacy Act, which requires regulated entities that hold personal information to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Sections 20Q and 21T of the Privacy Act impose equivalent obligations on credit reporting bodies and credit providers. Similarly, section 11(1) of the statutory Privacy (Tax File Number) Rule 2015 requires tax file number (**TFN**) recipients to protect TFN information from misuse and loss, and from unauthorised access, use, modification or disclosure.

48. On 6 June 2013, the House of Representatives passed the Privacy Alerts Bill with bipartisan support. On 17 June 2013, the Bill was introduced into the Senate and was referred on 18 June 2013 to the Legal and Constitutional Affairs Legislation Committee for inquiry. The committee reported on 24 June 2013, its sole recommendation being that the Senate pass the Privacy Alerts Bill. The Privacy Alerts Bill lapsed on prorogation of the 43rd Parliament.

Parliamentary Joint Committee on Intelligence and Security Reports

2013 Report

49. In May 2012, the then Government asked the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) to inquire into a package of potential reforms to Australia's national security legislation including a mandatory data retention regime for personal telecommunications data. The PJCIS reported a large number of the submissions to the inquiry objecting to data retention on information security grounds, including concerns about creating a 'honeypot' of information that would be vulnerable to a data breach[7].

50. In May 2013, the PJCIS released *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. The report recommended that, if a mandatory data retention regime should proceed, its introduction should include the introduction of a robust mandatory data breach notification scheme (Recommendation 42).

51. The Commonwealth Attorney-General's Department submitted to the inquiry that, if enacted, mandatory data breach notification laws could complement the current legislative security requirements and a data retention regime in a least four ways, by:

[7] *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Parliamentary Joint Committee on Intelligence and Security, Parliamentary Joint Committee on Intelligence and Security, 2013, pages 167-75.

1. mitigating the consequences of a breach;
2. creating incentives to improve security;
3. tracking incidents and providing information in the public interest; and
4. maintaining community confidence in privacy laws[8].

2015 Report

52. In November 2014, the Government referred the provisions of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (**Data Retention Bill**) to the PJCIS for inquiry and report. The PJCIS considered evidence provided by the Privacy Commissioner and others that, by creating a large repository of personal information, the proposed data retention scheme increases the risk and possible consequences of a data breach and that a mandatory data breach notification scheme is one way to manage the impact of any data breach on individuals[9].

53. In February 2015, the PJCIS released the Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (**PJCIS Report**). The PJCIS Report recommended the introduction of a mandatory data breach notification scheme by the end of 2015 (Recommendation 38). On 3 March 2015, the Government agreed to all recommendations of the PJCIS Report, including the introduction a mandatory data breach notification scheme. The Government stated it would consult on the draft legislation for the mandatory data breach notification scheme.

2015-16 consultation

54. In response to the Government's commitment to introduce a mandatory data breach notification scheme, the Attorney-General's Department drafted the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (**Serious Data Breaches Bill**). The Serious Data Breaches Bill was based on the Privacy Alerts Bill with changes made to decrease the regulatory burden and further accommodate the feedback received during 2012 and 2013.

55. On 3 December 2015 the Attorney-General's Department released a Discussion Paper on the proposal to introduce a mandatory data breach notification scheme and consulted on the Serious Data Breaches Bill and a draft Regulation Impact Statement (**RIS**) for the proposal for a 13 week period until 4 March 2016.

56. The Attorney-General's Department responded to stakeholder concerns about the proposed mandatory data breach notification scheme raised during the 2015 16 consultation by revising the Serious Data Breaches Bill. This revision resulted in the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (**Notifiable Data Breaches Bill**).

[8] *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Parliamentary Joint Committee on Intelligence and Security, 2013, pages 175.

[9] *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 2015, pages 293-5.

Status of the RIS at each major decision point

57. A RIS was prepared for the Privacy Alerts Bill that was assessed by the Office of Best Practice Regulation (**OBPR**) as meeting the Government's best practice regulation requirements. As indicated above, the Privacy Alerts Bill was introduced to Parliament in May 2013.

58. There was no RIS prepared in advance of the Government's commitment to introduce a mandatory data breach notification scheme in March 2015. However, the commitment was part of the Government's response, on 3 March 2015, to the PJCIS Report on the Data Retention Bill[10]. The Data Retention Bill was a package of reforms to prevent the further degradation of the investigative capabilities of Australia's law enforcement and national security agencies and was introduced to Parliament on 30 October 2014[11].

59. Subsequent to the Government's commitment to introduce a mandatory data breach notification scheme in March 2015, a RIS for the Serious Data Breaches Bill was prepared in advance of the decision to undertake the 2015-16 consultation. This RIS was submitted to the OBPR for early assessment. OBPR found the RIS suitable for consultation. In response to comments provided during the 2015-16 consultation the Serious Data Breaches Bill was redrafted as the Notifiable Data Breaches Bill.

What is the problem trying to be solved?

What a data breach is

60. Under the Data Breach Guide, a data breach is defined as the situation where 'personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference'[12]. The ALRC report noted that, with advances in technology, entities are increasingly holding larger amounts of identifying information in electronic form, raising the risk that a breach of this information could result in another individual using the information for identity theft and identity fraud. Stalking, embarrassment, or discrimination can also result from the unauthorised release or loss of information held by an agency or organisation. Currently, there is no mandatory requirement that an entity inform an individual following a data breach involving their personal information.

61. The Data Breach Guide notes that breaches are not limited to malicious actions, such as theft or 'hacking', but may arise from internal errors or failure to follow information-

[10] See at: https://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/Government-Response-To-Committee-Report-On-The-Telecommunications-Interception-And-Access-Amendment-Data-Retention-Bill.aspx.

[11] See at: https://www.attorneygeneral.gov.au/Mediareleases/Pages/2014/FourthQuarter/30October2014-TelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill2014.aspx.

[12] Data Breach Guide, page 2.

handling policies that cause accidental loss or disclosure. The Data Breach Guide provides some common examples:

- lost or stolen laptops, removable storage devices, or paper records containing personal information;
- hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased;
- databases containing personal information being ‘hacked' into or otherwise illegally accessed by individuals outside of the agency or organisation;
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment;
- paper records stolen from insecure recycling or garbage bins;
- an agency or organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address; and
- an individual deceiving an agency or organisation into improperly releasing the personal information of another person[13].

Why data breaches are a problem

62. As the collection of personal information by agencies and organisations increases the potential damage caused by data breaches increases. The potential damage includes damage to individuals, particularly through identity theft and crime, as well as the undermining of trust in the digital economy.

63. The ALRC found that, with advances in technology, agencies and organisations are storing vast amounts of identifying information electronically. The increased use of the internet and other current and emerging mobile technologies pose new challenges for privacy protection as Australians increasingly transact commercially and engage socially in the online environment. Personal information such as medical records, bank account details, photos, videos and details about individuals’ personal preferences and occupational history is increasingly transitioning to web pages and data centres, with varying degrees of accessibility and security.

64. A number of reports indicate that, whilst the threat of data breaches is becoming increasingly clear, many organisations are not protecting themselves from cyber-attacks. A 2014 Telstra cyber security report found 36% of organisations were unprepared for a security incident[14]. A 2015 survey of 5,244 IT and IT security practitioners, including 200 from

[13] Data Breach Guide, page 5.

[14] *Telstra Cyber Security Report 2014*, page 19.

Australia, found that 57% of respondents do not think their organisation is protected from advanced cyber-attacks and that 63% do not think their organisation could stop exfiltration of confidential information[15]. A 2015 survey of over 700 Chief Information Officers, Chief Technology Officers etc. found a significant decrease in the implementation of effective data leakage policies. For example, organisations that have a data protection and privacy policy dropped from 87% in 2013 to 58% in 2015[16].

65. APP 11 requires organisations that hold personal information to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. A breach of APP 11 would be an interference with the privacy of an individual and could be the subject of investigation by the Australian Information Commissioner as a result of a complaint from the individual or on the Commissioner's own initiative. Such an investigation can result in the Commissioner using his or her enforcement powers including powers to accept an enforceable undertaking, bring proceedings to enforce an enforceable undertaking, make a determination, bring proceedings to enforce a determination and to apply to the court for a civil penalty order for a breach of a civil penalty provision.

66. 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 $360,000 for individuals and $1,800,000 for bodies corporate.

67. However, whilst there are mechanisms in the Privacy Act to address the damage caused by data breach, organisations have no legal obligation to notify an individual if their personal information is breached (with the exception of eHealth information as discussed below). This is regardless of the sensitivity of the personal information and regardless of the risk of harm that may arise from the data breach.

68. The absence of a requirement to notify individuals of data breaches involving personal information does not align with the almost universal agreement from the Australian public that an organisation should inform them if their personal information is lost[17].

69. The Data Breach Guide promotes the notification of serious data breaches. However, it is voluntary. A key issue is whether the Data Breach Guide is operating as an effective means to encourage widespread notification of breaches. In submissions to the 2015-16 consultation the OAIC and the Centre for Internet Safety both indicated that serious data breaches are being underreported in Australia. As numbers cited above demonstrate, voluntary notifications have increased by 250% since 2009-10, from 44 to 110. However, the

[15] *Exposing the Cybersecurity Cracks: A Global Perspective Part 1*, Ponemon Institute, pages 2 and 9.

[16] *The Battle Continues: Working to Bridge the Data Security Chasm*, Protiviti, page 12.

[17] *Community Attitudes to Privacy survey Research Report 2013*, Office of the Australian Information Commissioner, 2013 (Community Attitudes Report), page 5.

OAIC predicts, based on comparisons with other jurisdictions, that notifications under a mandatory data breach notification scheme would nearly double to around 200.

70. Another issue with a voluntary scheme is potential inconsistency in how entities choose to participate. An example is a Privacy Commissioner investigation where an entity voluntarily notified a data breach three years after it occurred[18]. Although the Commissioner expressed concern about the significant delay between when the entity became aware of the data breach and when it chose to notify the breach, the Commissioner's current investigative and enforcement powers are based around requirements of the Privacy Act, and are not designed to deal with cases where a business's voluntary data breach notification practices possibly do not reflect community expectations.

71. This supports a conclusion that a continuation of voluntary data breach reporting will contribute to the extent of the data breach problem.

Identity theft and crime

72. Identity crime is amongst the most common and costly crimes in Australia, with an estimated annual economic impact of over $2 billion. Around 4-5 per cent of Australians experience identity crime each year that results in financial loss[19]. The Australian Government's National Identity Security Strategy (**NISS**) aims to prevent identity crime, assist victims to restore their compromised identities and to enhance the security and integrity of the systems used by government agencies to issue and maintain documents used by Australians as evidence of identity. The NISS supports a broad range of law enforcement, national security, government service delivery and broader digital economy policy objectives. This includes efforts to improve the systems and processes used to verify the identities of people seeking to transact with government agencies and other organisations with legislative requirements such as financial institutions or others with a reasonable need to verify a person's identity, such as recruitment agencies.

73. One of the key NISS initiatives is the Document Verification Service (DVS) which enables government agencies and private sector organisations to match biographic information on identity documents, such as driver licences and passports, against the records of the document issuing agency. The DVS is undoubtedly strengthening the ability of both government and the private sector to combat identity crime, by making it harder for criminals to use documents with fictitious identity information. However it does not prevent criminals using stolen information used on legitimately issued identity documents and substituting their own photos. Law enforcement agencies are already detecting cases of high quality fraudulent identity documents using this methodology – documents that would pass a DVS check. Preventing this type of fraud can be assisted by greater use of biometrics.

[18] See at: https://www.oaic.gov.au/media-and-speeches/statements/catch-of-the-day-data-breach.

[19] Attorney-General's Department, Identity Crime and Misuse in Australia 2013-14, p4 at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-Australia-2013-14.pdf.

74. The Attorney-General's Department is establishing a facial biometric matching capability to facilitate sharing and matching of facial images from existing records between those agencies with a lawful basis to do so. This will assist agencies to protect people from identity theft, and help victims restore their compromised identities. However the system will only be available to government agencies (at least for the foreseeable future) and will need to be complemented by other risk mitigation measures, such as a mandatory notification scheme.

75. There is a link between the breach of personal information and identity theft and crime. A report released in 2014 indicated data breaches, whether accidental or deliberate, present significant opportunities for obtaining personal identifiable information that is used in identity crime. The types of personal information used to commit identity crime are increasingly being collected and stored in databases held by a variety of government agencies and private sector organisations and the aggregation of this information, particularly in electronic forms that are accessible online, increases the risk that information may be acquired through data breaches, either accidentally or through deliberate attempts to steal personal information[20].

76. Identity theft involves the acquiring or collecting of an individual's personal information for criminal purposes. A 2015 review of data breaches found 53.2% of data breaches in the first half of 2015 were caused by identity theft amounting to 74.9% of compromised data records[21]. Stolen data was used for criminal purposes in the majority of data breach incidents[22].

77. Stolen data is available for sale on dark web marketplaces. The type of data available includes PayPal and credit card accounts, bank log-in credentials and personal information including names, addresses, dates of birth and other information. Personal information is often traded in the form of scans of documents like passports, driver licences etc[23].

78. In its submission to the 2015-16 consultation IDCARE, Australia and New Zealand's national identity support service, provided revealing statistics on the trade in identifying information. A physical Australian State or Territory Driver Licence, which is depended upon most by hackers and identity thieves, has a value of $417-$450 on the dark web marketplace Agora, whilst a physical Australian Passport has a value of $5110.

79. Any breach of the secure storage of personal information an entity holds may be sufficient to allow an unauthorised person to assume the identity of the victim and use that illicit identity to open, for example, new accounts in the victim's name. A stolen identity can

[20] *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot,* Attorney-General's Department, 2014, page 23.

[21] *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot,* Attorney-General's Department, 2014, page 23.

[22] *Following the Data: Dissecting Data Breaches and Debunking Myth*s, Huq, Numaan, page 7.

[23] *Following the Data: Dissecting Data Breaches and Debunking Myths*, Huq, Numaan, pages 15-37.

be used to commit identity fraud where a fabricated, manipulated or stolen identity is used to gain a benefit or avoid an obligation[24]. In its submission to the 2015-16 consultation IDCARE stated that of the most recent 2,500 cases it managed where identifying information was reportedly breached, 32% of individuals detected a further misuse of this information, for example the exploitation by criminals of the identifying information.

80. Under the voluntary system, the notification of individuals can be delayed for years, as discussed above. Such a failure to notify an affected individual of a data breach in a timely manner increases the potential cost of the data breach on the individual. For example, a delay in notification increases the risk of an affected individual becoming a victim of an identity crime such as identity theft, as they may be unaware of the need to take action to mitigate the detrimental consequences of the data breach. Summary statistics for the last 12 months presented in IDCARE's submission to the 2015-16 consultation indicated that the average number of days between a data breach and an individual being notified of the breach was 405 days, whereas the average time between a data breach and the misuse of compromised information was 72 hours.

Underreporting of data breaches to individuals

81. There is a lack of empirical evidence on whether data breaches are being underreported to individuals as well as regulators. Submissions to the 2012 consultation and 2015-16 consultation varied on whether there is an underreporting of data breaches to the individuals to whom the data relates. However, given the link outlined above between data breach and identity theft and crime, an underreporting of data breach to the individuals to whom the data relates has the potential to cause harm to those individuals as it would deny them the opportunity to mitigate against any possible harm caused by the breach. As outlined above the harm from identity theft and crime can have significant financial and health impact on individuals.

82. The Privacy Commissioner has publicly stated that, based on media reports citing information technology security experts, that individuals and the OAIC have likely only been notified of a small percentage of data breaches that are occurring[25].

83. In its submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Privacy Alerts Bill the OAIC provided evidence suggesting that in instances of admitted data breach 18% of interviewed organisations did not notify anyone outside the organisation of the data breach and 68% did not notify affected customers of the data breach[26].

---

[24] ALRC Report, paragraph 51.4.

[25] See, for example, at: https://www.oaic.gov.au/engage-with-us/submissions/mandatory-data-breach-notification-discussion-paper-submission-to-attorney-general-s-department and https://www.oaic.gov.au/engage-with-us/submissions/inquiry-into-privacy-amendment-privacy-alerts-bill-2013.

[26] See: https://www.oaic.gov.au/engage-with-us/submissions/inquiry-into-privacy-amendment-privacy-alerts-bill-2013.

84. In its submission to the 2015-16 consultation the OAIC stated that without mandatory reporting of data breaches, some entities may not notify individuals that may be affected, or the OAIC. The OAIC suspects that many Australian entities do not voluntarily report all data breaches or recognise which incidents they should report and that data breaches regularly come to the OAIC's attention through the media and allegations from third parties rather than through notification by the entities.

85. In its submission to the 2012 consultation, the Centre for Internet Safety also asserted that significant amounts of underreporting had been occurring and that the voluntary system was not working. A number of submission to the 2015-16 consultation agreed that data breaches are underreported in Australia. These conclusions were supported by the relatively low number of notifications occurring under the current voluntary scheme compared with notifications in other jurisdictions and the fact that the low number of voluntary notifications contrasts with data breach trends being reported.

86. In its submission to the 2015-16 consultation IDCARE stated that the relatively small number of data breaches reported to the Commonwealth Office of the Australian Information Commissioner would suggest that much more work needs to be done to educate reporting entities on the real risks and harm caused from the unauthorised disclosure or loss of identifying information.

87. Importantly, statistics provided by IDCARE suggest that the content of voluntary notifications may be inadequate. IDCARE stated only 11% of organisations from a sample of 221 organisations within IDCARE's response library provided online guidance to impacted individuals about what they could do to mitigate harm following the compromise of their information.

88. On the other hand, some respondents to the 2012 consultation argued that the lack of clear information about the level of underreporting shows that there is no evidence of regulatory or market failure that has created a consumer protection risk warranting a response. A number of respondents to the 2015-16 consultation including the Association for Data-Driven Marketing and Advertising, the Interactive Games and Entertainment Association and the Digital Industry Group Inc. maintained that the voluntary data breach reporting scheme is sufficient.

The magnitude of data breaches

89. Studies and anecdotal evidence suggest that breaches of data security are increasing in frequency and scope. A 2014 Australian report found nearly a quarter of businesses surveyed had suffered an IT security breach in the previous 12 months, and 60% had suffered a breach in the previous five years[27]. A PwC report found 38% more security incidents were detected in 2015 than in 2014[28].

[27] *Telstra Cyber Security Report 2014*, page 30.

[28] *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016*, PwC, page 24.

90. There have been a number of recent high profile data breaches that have highlighted the magnitude of the issue. Examples from Australia and abroad include:

a. In 2012, 6.5 million encrypted passwords for LinkedIn users were the subject of a data breach as a result of unauthorised access and disclosure of the information. More than 100 million email and password combinations of LinkedIn members that were stolen in the 2012 breach were subsequently released on line in May 2016[29].
b. In October 2013, Adobe reported that it had been the target of a cyber-attack that affected at least 38 million Adobe customers globally, including over 1.7 million Australians[30].
c. In June 2014, Optus reported 3 separate data breaches where the security of the personal information of over 300,000 of its customers was compromised[31].
d. In February 2014, a data breach at the Department of Immigration and Border Protection compromised the personal information of approximately 10,000 asylum seekers[32].
e. In November 2014, a hacking incident at Sony Pictures Entertainment was discovered that involved the personal information of employees, including social security and health information, as well as other Sony corporate information[33].
f. In June 2015, the Privacy Commissioner finalised enquiries into a data breach of Australian online retailer Catch of the Day, expressing concern that the data breach, which occurred in May 2011, had not been notified to the Commissioner until June 2014[34].
g. In July 2015, the US Office of Personnel Management outlined details of two data breaches that compromised personal information about more than 21.5 million current and former US Government employees and other individuals[35].
h. In July 2015, client data from dating website Ashley Madison was stolen and published online in August 2015. Media reports about the number of affected Australians range from 460,000–900,000. On 24 August 2016 the Australian Privacy Commissioner released a joint finding with the Privacy Commissioner of Canada highly critical of the dating website's privacy and personal data security practices[36].

[29] LinkedIn Official Blog: *Protecting Our Members*, available at https://blog.linkedin.com/2016/05/18/protecting-our-members.

[30] See at: https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/adobe-omi.

[31] See at: http://www.oaic.gov.au/privacy/applying-privacy-law/enforceable-undertakings/singtel-optus-enforceable-undertaking.

[32] See at: https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/dibp-omi.

[33] See Sony Pictures Entertainment's notification to affected individuals (made in accordance with Californian mandatory data breach legislation) at: http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf.

[34] See at: https://www.oaic.gov.au/media-and-speeches/statements/catch-of-the-day-data-breach.

[35] See at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/.

[36] See at: https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison.

i. In September October 2015, retailers Kmart and David Jones disclosed that their online stores experienced data breaches compromising names, email and postal addresses and order details of some customers. Both retailers publicly announced the breaches, voluntarily notified the AFP, the OAIC and affected individuals, and engaged expert IT security advice. In both cases the OAIC stated it would await further information from the retailers and praised the voluntary notification of the breaches[37].

91. There are numerous reports providing details of the magnitude and costs of data breaches and the linked issue of identity crime. One 2015 report that collected data breach information from 70 organisations in 61 countries identified 79,790 security incidents and 2122 confirmed data breaches. It reported an overall cost of $400 million from the 700 million compromised records[38]. Another global report identified 312 breaches, with 348 million identities exposed, with an average of 1.1 million average identities exposed per breach[39]. A recent report estimated that $US16 billion was stolen from 12.7 million identity fraud victims in the U.S in 2014[40].

Who data breaches affect

92. The impact of data breaches and related identity theft and crime is widespread and affects businesses, individuals and government agencies.

93. A 2016 report specific to Australia commissioned by IBM and conducted by the Ponemon Institute assessed the cost of 26 government and non-government data breaches from 11 industry sectors and found the average total cost of a data breach to business was $2.64 million with a cost of $142 per lost or stolen record[41]. It appears that a considerable proportion of data breaches involve the loss or theft of personal information that is ultimately used in identity crime. A US study found that two-thirds of identity fraud victims in 2014 had previously received a data breach notification in the same year[42].

94. Identity crime is one of the most prevalent types of crime affecting Australians. A report on the results of a 2014 Australian Institute of Criminology survey estimated the national economic impact of identity crime in 2014 to be $AUD2.4 billion. It found 8.9 percent of people surveyed experienced criminal misuse of their personal information in the previous 12 months and spent an average of 15.3 hours dealing with the consequences of

[37] See at: https://www.oaic.gov.au/media-and-speeches/statements/kmart-australia-data-breach and https://www.oaic.gov.au/media-and-speeches/statements/david-jones-data-breach.

[38] *2015 Data Breach Investigations Report*, Verizon (Verizon Report), page 1.

[39] Internet Security Threat Report 20: Symantec, pages 78-81.

[40] 2015 Identity Fraud: Protecting Vulnerable Populations, Javelin Strategy & Research, 2015. See at: https://www.javelinstrategy.com/coverage-area/2015-identity-fraud-protecting-vulnerable-populations.

[41] *2016 Cost of Data Breach Study: Australia*, Ponemon Institute (Ponemon Report), page 1.

[42] *2015 Identity Fraud: Protecting Vulnerable Populations*, Javelin Strategy & Research, 2015.

having their personal information misused. Almost five percent of those surveyed reported actual out of pocket losses as a result of the misuse of their personal information. These out of pocket losses averaged $3,572 per incident. The survey found nearly 12 percent of individuals whose personal information was misused in the previous 12 months experienced mental or physical health impacts that led to them seeking counselling or other treatment[43].

95. In its submission to the 2015-16 consultation IDCARE indicated that around one in five IDCARE clients present psychological or somatic symptoms and impacts following the compromise of their personal information with the most common impacts being heightened anxiety, depression and feeling uncommunicative.

Community expectations

96. According to a 2013 national privacy survey conducted by the OAIC, the security of personal information, particularly on the internet, concerns the majority of Australians[44]. Eighty-nine per cent of respondents worried about the security of their personal information when using the internet, 69% did not trust social media services to protect their information and, 8% avoided using credit cards online due to concerns about the security of their personal information.

97. The survey also found that two-thirds of Australians are concerned that they may become a victim of identity theft and fraud in the next year, and one third say that they have had problems with the way that their personal information was handled in the previous year. The survey identified that over 90% of the Australian public thinks that both government and private business organisations should inform them if their personal information is lost and how they protect and handle personal information in the first place.

Current data breach requirements

<u>My Health Records Act</u>

98. At present in Australia, mandatory data breach notification requirements apply only in the event of unauthorised access to certain eHealth information under the *My Health Records Act 2012* (**My Health Records Act**). Under the My Health Records Act, certain participants (the System Operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider) are required to report data breaches that occur in relation to the eHealth record system to the OAIC and the System Operator. Failure to report a data breach could be a breach of the My Health Records Act, and penalties may apply.

<u>Voluntary data breach notification scheme</u>

[43] *Identity crime and misuse in Australia: Results of the 2014 online survey*, Australian Institute of Criminology Research and Public Policy Series 130, pages iii, xi, 22.

[44] *Community Attitudes to Privacy survey Research Report 2013*, Office of the Australian Information Commissioner, 2013 (Community Attitudes Report), pages 3–5.

99. In the absence of a legal requirement, entities are encouraged to adhere to the Data Breach Guide. The Data Breach Guide outlines key steps and factors agencies and organisations should consider when responding to a data breach involving personal information that they hold. The Data Breach Guide provides advice around obligations under the Privacy Act to put in place reasonable security safeguards and to take reasonable steps to protect the personal information that they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. Depending on the circumstances, those reasonable steps may include the preparation and implementation of a data breach policy and response plan.

100. The OAIC guide contains 4 key steps for an agency or organisation to take when a data breach occurs. These are:

1. contain the breach and do a preliminary assessment;
2. evaluate the risks associated with the breach;
3. undertake notification (if appropriate); and
4. prevent future breaches.

Why is government action needed?

101. APP 11 of the Privacy Act obliges regulated entities to take reasonable steps to maintain the security of the personal information they hold, while other provisions create equivalent obligations in regard to other kinds of information. However, the Privacy Act does not oblige entities to notify individuals whose personal or other information has been compromised. Entities that do not participate in the voluntary scheme face no legal sanction.

102. As outlined above there are concerns that under the current voluntary notification system data breaches are being underreported or notification is being delayed to the individuals to whom the breached information relates and that this affects an individual's ability to take steps to mitigate any possible harm associated with the breach. Given the link between data breaches and identity theft and crime outlined above, these possible issues with the voluntary notification system may be contributing to the cost associated with identity theft and crime.

103. The OAIC's view is that notification may be a 'reasonable step' where a data breach has occurred (with 'reasonable step' being a key term used in APP 11 and other Privacy Act security provisions mentioned above). However, it believes an express mandatory data breach notification law would provide agencies and organisations with greater clarity and certainty regarding their obligation to notify, and the circumstances in which notification should be made. The OAIC believes that a mandatory notification scheme is necessary to:

- give confidence to all Australians that if they are affected by a data breach, they will be given a chance to protect their interests; and

- signal to entities that protection of individuals' personal information should be a priority in the digital age.

104. The Privacy Act's information security requirements are aimed at encouraging entities to take reasonable steps to minimise the possibility that personal information could be compromised. Provided an entity meets these requirements, it would not be in breach of its existing Privacy Act obligations, even if it suffered a data breach involving large amounts of personal information.

Does the Government have the capacity to successfully intervene?

105. In terms of whether a mandatory notification scheme would operate to limit the harmful effects of a data breach, some private sector stakeholders in responses to the 2012 consultation and in the 2013 targeted consultation process queried whether there was empirical evidence to suggest that notification of itself has been effective in reducing the likelihood or impact of a data breach in overseas countries.

106. A number of respondents to the 2015-16 consultation including PwC, Electronic Frontiers Australia and the OAIC stated that a mandatory data breach notification scheme would assist in reducing the damaging effects of the data breach.

107. US cases are limited but provide some evidence on this issue. Of the limited studies to date, there is empirical evidence to show that notifying affected consumers can reduce harmful effects such as identity theft. A 2008 study appeared to show that connection between data breaches and identity theft does exist. In that paper, a study of US jurisdictions using data from between 2002 and 2007 showed that the adoption of data breach notification laws 'reduce the identity theft rate by just 2%, in average'. Although this figure may seem low, a 1.8% reduction in identity theft would lead to savings of approximately $US1 billion. When that study was updated in 2011, the conclusion was that, based on data from 2002 to 2009, an empirical analysis revealed that these laws have reduced identity thefts by about 6.1%[45]. It is therefore open for the conclusion to be drawn that data breach laws are a longer term effective measure in combating identity theft.

108. It is difficult to determine whether or to what extent mandatory data breach notification would produce similar results in Australia. However, if introduction curbed identity theft to the same extent as the US study results in the long term, the Australian Institute of Criminology figures cited above suggest savings of $AUD146 million per annum.

What is the alternative to Government action?

109. The alternative to government action is the maintenance of the current voluntary data breach notification scheme and its associated under-reporting of data breaches to individuals to whom the personal information breached relates. This alternative to action could see the costs of data breaches to organisations, government and individuals continuing to increase.

[45] 'Do Data Breach Disclosure Laws Reduce Identity Theft? (Updated)', Sasha Romanosky, Rahul Telang and Alessandro Acquisti, Journal of Policy Analysis and Management, Vol. 30, No. 2, pp. 256-286, 2011. See at: http://www.econinfosec.org/archive/weis2008/papers/Romanosky.pdf.

110. The Ponemon Report estimates the costs to businesses of data breaches have increased from $123 per compromised record in 2010 to $142 per compromised record in 2016 amounting to a total organisational cost of data breaches rising from $1.97 million in 2010 to $2.64 million in 2016. The cost associated with the business losses from data breach, such as abnormal turnover of customers, reputation losses and diminished goodwill, increased from $0.66 million in 2010 to $0.84 million in 2016[46].

111. As already outlined, information from the Australian Institute of Criminology and IDCARE, data breaches and associated identity theft and crime has a significant financial and health impact on individuals.

What are the objectives of Government action?

112. The objectives of a mandatory data breach notification scheme accord with the objectives of the Privacy Act. The objective of the Privacy Act is to promote the protection of privacy of individuals, while recognising that this protection should be balanced with the interests of entities carrying out their legitimate functions or activities. Government action will provide certainty and consistency to organisations and agencies when responding to data breaches.

113. The key objective of mandatory data breach notification scheme is to allow individuals whose personal information had been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach. The ALRC believed that, by arming individuals with the necessary information, they will have the opportunity to take appropriate action, such as monitoring their accounts or taking preventative measures such as changing passwords and cancelling credit cards.

114. A key outcome of a well-balanced privacy framework is the provision of a safer and more transparent environment for Australians to entrust their personal information to agencies and organisations. Greater assurance about the safety of personal information will encourage consumers to more fully engage in e-commerce, thereby boosting Australia's digital economy.

115. Another goal of privacy policy is to enable an enhanced information and assessment process to better inform policy makers, regulators, law enforcement and researchers about trends in the handling of personal information. Among other things, mandatory data breach notification will provide the OAIC with information about trends in data breaches that may assist in the development of useful guidance material for entities about information security.

116. A mandatory data breach notification scheme would also likely result in an improvement in compliance with privacy obligations: the reputational damage that can follow a high-profile data breach, and the commercial consequences of such a breach, can provide powerful incentives to improve security. On the other hand, reputational damage is often cited as a reason why some private sector organisations do not notify regulators or affected individuals about data breaches.

[46] Ponemon Report, page 2-3.

117. Evidence suggests this concern is valid to some extent: the Ponemon Report found that the biggest financial consequence to organisations of data breach is lost business. The same report found that the cost of a data breach is lower for companies that have strong information security policies in place before a data breach occurs[47]. A 2016 Deloitte survey conducted in Australia found that 29% of survey respondents who had received a voluntary data breach notification trusted the notifying entity less. Importantly, however, these respondents were outweighed by the 33% of respondents who actually trusted the entity more, presumably because of the transparency shown in undertaking notification. Additionally, the Deloitte survey shows that a significant 71% of people who had been informed of a breach did not trust the organisation any less following the notification[48]. A 2016 report by the Rand Corporation on a survey of consumer attitudes to data breaches in the U.S. found that 11 percent of respondents stopped dealing with a company following a breach. Of the 89% who chose to remain with the company, 23% said they gave them less business than before and one percent gave them more business than before the breach[49].

118. Given the figures from the OAIC's 2013 national privacy survey cited above showing strong community support for data breach notification, the potential loss of trust following a notification would also need to be balanced against the possible reputational risk of not notifying a data breach that later comes to light.

119. A mandatory scheme would also encourage agencies and organisations to be transparent about their information-handling practices. This would support the operation of existing APP 1 in the Privacy Act, which requires entities to make available a clearly expressed and up-to-date policy about how the entity manages personal information.

What policy options are being considered?

Option One – Retain the status quo

120. Option One is to maintain the status quo. This means that entities subject to the Privacy Act will have no legal obligation to report a breach of personal information except in relation to My Health Records Act. They will continue to be obliged under the Privacy Act to secure personal and other specific kinds of information they hold, and will continue to be encouraged to comply with the existing OAIC Data Breach Guide.

121. The Data Breach Guide will continue to provide general guidance on key steps and factors for agencies and organisations to consider when responding to a data breach involving the personal information that they hold. Entities will also be able to draw on other relevant OAIC guidance material, such as the APP Guidelines[50], which provide advice about key terms in the Privacy Act, as well as compliance with APP 11, and the *Guide to Securing*

[47] Ponemon Report, page 1–2.

[48] *Deloitte Australian Privacy Index 2016: Trust Without Borders*, Deloitte, 2016 (Deloitte Report), page 11.

[49] *Consumer Attitudes Towards Data Breach Notifications*, Rand Corporation, page 26.

[50] See at: http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/.

Personal Information[51], which provides advice about 'reasonable' information security steps under the Privacy Act. This guidance material expresses the view that, depending on the circumstances, reasonable steps may include the preparation and implementation of a data breach policy and response plan (that includes consideration of whether to notify affected individuals and the OAIC).

122. In response to the 2012 consultation and the 2015-16 consultation, a number of private sector stakeholders argued that the voluntary scheme was sufficient in encouraging the reporting of significant breaches and in giving guidance to entities about how to effectively respond to these breaches. Many argued that private sector organisations have developed good privacy practices since the application of the Privacy Act to the private sector in 2001, and understand the importance of seeking the assistance of the Privacy Commissioner where appropriate and in dealing with the privacy concerns of their customers. They also argued that, contrary to anecdotal reports, there is no real evidence in Australia of underreporting of significant data breaches to the OAIC. Additionally, some argued that mandatory data breach notification laws effectively penalise regulated entities, which are often the targets of cybercrime attacks.

123. Maintaining the status quo would also allow the market participants to continue to develop good privacy practices consistent with the expectations of their customers. It is arguable that there is a sufficient commercial incentive for organisations to implement good privacy practice and notify their customers in the event that their information may become compromised. The reputational costs that come with failing to respond properly to significant data breaches are a strong incentive to notify the OAIC and consumers about breaches. In the current digital economy, consumers are more likely to consider the privacy track record and policies of a business when deciding whether to entrust it with their personal information[52].

124. The Information Commissioner has an existing power under the Privacy Act to audit private sector organisations which could be used to investigate actual or suspected data breaches (for example, following complaints from affected individuals, media articles or other information). This has the potential to make it more difficult for an entity to hide a data breach. For reputational risk reasons, the possibility of being audited provides the incentive to report data breaches to the Commissioner and affected individuals proactively.

Option Two – Introduce a mandatory data breach notification scheme

125. Option Two is to amend the Privacy Act to introduce a mandatory data breach notification scheme that requires entities to report notifiable data breaches to the OAIC and to affected individuals. A notifiable data breach is one that would lead a reasonable person to conclude that there is a likely risk of serious harm to any of the individuals to whom the breached information relates, where no exceptions to notification apply. Option Two will

[51] See at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information.

[52] *Privacy and the Internet: Australian Attitudes Towards Privacy in the Online Environment*, Centre for Internet Safety, 2012, page 1.

make no changes to the mandatory notification scheme operating under the My Health Records Act.

126. Considerable consultation has been undertaken with stakeholders on the design of an amendment to introduce a mandatory data breach notification scheme. Following the 2012 consultation on the introduction of a mandatory data breach notification scheme the Attorney-General's Department drafted the Privacy Alerts Bill which was the subject of the 2013 targeted consultation. The Privacy Alerts Bill provided the basis for the Serious Data Breach Notification Bill, which was the subject of the 2015-16 consultation. To respond submissions received in the 2015-16 consultation the Serious Data Breaches Bill was redrafted as the Notifiable Data Breaches Bill in 2016.

Who should Option Two apply to?

127. There was broad consensus from submitters to the 2012 consultation, the 2013 targeted consultation and the 2015-16 consultation which entities should be subject to the scheme, with most submitters who commented agreeing with the ALRC's view that it should apply to entities currently regulated by the Privacy Act. A small number of submitters argued that all businesses that hold personal information should be subject to the scheme, or that, if the Government removed or amended exemptions in the future (e.g. small businesses, political parties), those entities should also automatically be subject to the scheme.

128. The proposed model has reflected these comments by only applying the data breach notification law to entities currently regulated by the Privacy Act. The proposed model would not include entities, or some of their activities, that fall within exemptions in the Privacy Act, such as political parties, media organisations and most small businesses.

Notification threshold

129. Under the proposal, a notifiable data breach occurs following unauthorised access to, disclosure of, or loss of, personal or other specific kinds of information about an individual, where a reasonable person would conclude that the access, disclosure or loss would be likely to result in serious harm to that individual, and no exceptions to notification apply. This is consistent with the ALRC's recommended trigger for notification, which was a test based on a 'real risk of serious harm' to an affected individual.

130. The vast majority of submitters to the 2012 consultation who commented on the possible design of a mandatory scheme were in favour of the ALRC's recommended trigger for notification, or a variation of that test, i.e. a test based on a 'real risk of serious harm' to an individual. This would not require entities to report less serious privacy breaches to affected individuals or the OAIC.

131. However, in the 2013 targeted consultation and the 2015-16 consultation support was expressed for more explanation about, or a definition of what constitutes, 'a real risk of serious harm'. Without this additional assistance, it was argued that some regulated entities may adopt a more risk adverse approach to notification by taking a narrow interpretation that could lead to notification fatigue and create resourcing issues at the OAIC.

132. To address this concern, the proposed model:

a. modifies the ALRC's 'real risk of serious harm' threshold by introducing well-known legal concepts that involve an objective 'reasonable person' element and a reference to 'likely risk' rather than 'real risk' — retaining the core elements of the ALRC's recommended test while improving ease of compliance for regulated entities.

b. has an exception providing that notification is not required if a reasonable person would conclude that serious harm is not likely as a result of remedial action taken by the entity; and

c. provides a list of relevant matters, including encryption, when determining whether a reasonable person would conclude that there is a likely risk of serious harm to an individual.

133. The notification requirement under Option Two would apply to personal information held by APP entities, credit reporting information held by a credit reporting body, credit eligibility information held by credit providers, and tax file number information held by file number recipients. Where these types of information have been disclosed to foreign recipients, the requirement to notify in the event of a relevant data breach by the foreign recipient will remain with the disclosing Australian entity in certain circumstances.

When is notification required?

134. Option Two also provides that an entity should be required to notify as soon as practicable after it becomes aware of a notifiable data breach. This is in accord with the consensus amongst submitters to the 2012 consultation, the 2013 targeted consultation and the 2015-16 consultation who believed that flexibility, rather than a set time frame, was needed given the variable factors unique to each data breach. Where an entity is unsure of whether a serious data breach has occurred, Option Two also explicitly provides the entity with time to investigate the circumstances of the incident to determine whether notification is required (with no further action required if the notification threshold has not been met).

135. Option Two enables the Information Commissioner to provide an exemption, or a temporary deferral, to an entity from the requirement to notify a data breach. Submissions to the 2015-16 consultation supported the provision of additional flexibility to the Information Commissioner to consider the broader circumstances of an entity and a data breach. To address this concern, Option Two provides that the Information Commissioner can provide an exemption, or a temporary deferral, to an entity from the requirement to notify where the Information Commissioner is satisfied that it is reasonable in the circumstances to do so, having regard to the public interest.

136. Option Two contains a notification exception applying to all entities in cases where a law enforcement body, the Australian Security Intelligence Organisation or the Australian Signals Directorate advises the entity not to notify a notifiable data breach, or to delay notifying a notifiable data breach, because it would prejudice an enforcement related activity or raise national security concerns.

137. Option Two would also allow the Information Commissioner to direct an entity to notify a data breach. This power is primarily intended to operate in cases where an entity fails to comply with the mandatory notification requirement of its own volition. An entity would be able to seek review, at the Administrative Appeals Tribunal, of an Information Commissioner decision to issue a direction.

138. Submissions to the 2015-16 consultation supported a right of reply by entities to the Information Commissioner before such a direction is made. To address this concern, the proposed model now contains a requirement that the Information Commissioner must consult with an entity before making such a direction and give the entity an opportunity to either voluntarily notify the data breach or to contend that no data breach in fact occurred.

Who must make the notification?

139. The ALRC recommended that the entity involved in the breach should have the responsibility of notification. Most respondents to the 2012 consultation generally favoured this approach, noting that the entity was best placed to assess the breach, the adverse risks that might arise, and what mitigating action could be taken. Option Two incorporates this approach.

140. A number of submissions to the 2015-16 consultation referred to situations when more than one entity simultaneously 'holds' personal information that is subject to a breach: for example, if the information is stored in a joint database over which both entities have constructive possession, or if a particular form of subcontracting arrangement is involved. To address this situation the proposed model provides entities with the discretion to decide either which entity shall notify the notifiable data breach, or whether both of the entities should jointly notify (for example, by providing contact details for one or both entities in the notification).

Who should be notified?

141. Submissions to the 2015-16 consultation suggested that a requirement to notify all individuals whose information was subject to unauthorised access, unauthorised disclosure or loss in a notifiable data breach is unduly burdensome in cases where an entity is able to efficiently identify which individuals from a larger cohort are at risk of serious harm (for example, if the potential harm involves financial loss, and the entity only had payment details for a small number of individuals whose personal information was breached). To address this Option Two provides entities with the discretion to notify only individuals who a reasonable person would conclude are (or are assumed to be) at likely risk of serious harm as a result of a data breach, if it is practicable for the entity to identify those individuals.

Means of notification

142. During the 2012 consultation, the 2013 targeted consultation and the 2015-16 consultation there was general support from stakeholders for the proposition that the means of notification should be directly by phone, letter, email, in person, or by the normal means of communication between the entity and the individual. In the 2013 targeted consultation,

industry groups expressed the wish for flexibility so that regulated entities could notify individuals in a variety of ways.

143. Option Two incorporates a flexible approach to notification as it provides entities with the ability to notify an affected individual using the methods of communication it would normally use to contact the individual. 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.

144. Furthermore, should it be impossible or impracticable for the entity to notify each individual, the proposal does not require direct notification but rather requires the entity to publish the notification on its website (if any), and to take reasonable steps to publicise the notification. This will ensure that entities are not required to notify each affected individual if, for example, it would be impracticably expensive to do so. It also recognises that different kinds of notification techniques will be appropriate for different kinds of entities and data breaches (for example, it may be reasonable for some entities to publish information about a data breach via social media, whereas for others a newspaper advertisement may be reasonable).

Content of notification

145. The ALRC report recommended that, as a minimum, the notification should contain: a description of the breach; a list of the types of personal information that were disclosed; and contact information for affected individuals to obtain more information and assistance.

146. Submissions to the 2012 consultation provided a range of views on the content of notifications. In general, private sector submitters preferred less detailed information having to be provided, while privacy regulators/advocates believed more should be included. For example, Telstra believed it should be limited to the fact of the data breach, the information accessed/disclosed and what affected persons could do to minimise the impacts. On the other hand, the NSW Privacy Commissioner believed it should also include more details about the incident, the action that has been taken as a result of the breach and contacts at the agency or organisation.

147. The Notifiable Data Breaches Bill incorporates these suggestions, requiring a notification to contain the name and contact details for the entity notifying, a description of the breach, the kinds of information concerned and recommendations about the steps that individuals should take in response to the serious data breach. These requirements are based on the existing OAIC voluntary standards.

148. Submissions to the 2015-16 consultation from the Department of Immigration and Border Protection and the Department of Employment expressed the desirability of guidance material from the OAIC on the recommendations about the steps that individuals should take in response to the serious data breach. It is expected that the OAIC would provide guidance material on a mandatory data breach notification scheme.

149. Where the Information Commissioner directs an entity to notify a data breach, the Commissioner would also have discretion to direct the entity to include other information

about the data breach in the notification. This discretion has been included because it is expected that the power to compel notification would be used where an entity has failed to voluntarily notify a data breach, in which case it may be appropriate in some cases to include additional information in the notification (such as information about complaint mechanisms available under the Privacy Act).

Failure to notify

150. The Commissioner's power to direct an entity to notify a data breach is expected to be the most likely first regulatory response in the event that an entity fails to comply with its mandatory notification obligations.

151. Option Two would also link into the existing penalty structure in the Privacy Act, where (should the direction power prove inadequate, or where a further regulatory response is appropriate) less severe sanctions could be used before elevating to a civil penalty. These less severe sanctions could follow a Commissioner investigation and 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.

Option Three — Encourage industry to develop industry codes

152. Option Three is to encourage entities regulated under the Privacy Act to develop industry codes that provide a self-regulatory framework tailored to particular industry needs, taking into account existing reporting requirements and compliance issues. This could be complemented with increased efforts on the part of the OAIC to promote more awareness about the Data Breach Guide. This proposal would be assisted by OAIC guidance material, specifically its Guidelines for Developing Codes (**Code Guidelines**). Some industry groups have developed self-regulatory codes as a tool to promote standard practices and compliance.

153. The Ponemon Report found that the per capita cost of data breach incidents is different for particular industries, with financial, services, technology and energy companies incurring higher costs[53]. This finding is borne out in a separate 2016 Ponemon Report analysing worldwide data breach trends, though Ponemon found that healthcare and education entities experienced the highest data breach costs internationally[54]. Findings such as these may support the argument that particular industries are in a better position to identify what is reasonable in terms of developing their own data breach responses, having regard to their own compliance cost issues.

154. On the other hand, there were mixed views provided by key Australian industry groups in the 2013 targeted consultation process. Some believed that there would be no disproportionate adverse impact on different industry groups, while others believed that small

[53] Ponemon Report, page 2.

[54] *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute, page 2.

businesses (i.e. those subject to the Privacy Act because they trade in personal information, or are health service providers) would be affected in that way.

155. Under Part IIIB of the Privacy Act, the Information Commissioner can approve and register enforceable codes which are developed by entities on their own initiative or on request from the Commissioner, or developed by the Commissioner directly. An entity (or a body or association representing them) can develop a written code of practice for the handling of personal information that sets out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code.

156. An entity bound by a registered code must not do an act, or engage in a practice, that breaches that code and a breach of a registered code will be an interference with the privacy of an individual under the Privacy Act and subject to investigation by the Information Commissioner. While the Privacy Act allows the development of codes which would allow particular industries to develop a more tailored approach to personal information-handling, these cannot derogate from minimum standards set out in the APPs.

157. Option Three would be complemented with increased efforts on the part of the OAIC to promote more awareness about the OAIC guide, and the importance of complying with it as good privacy practice. Furthermore, the OAIC's *Guide to Securing Personal Information* and *Privacy Management Framework: Enabling Compliance and Encouraging Good Practice* contains suggested standardised rules that may help industry to adopt a self-regulatory framework.

What is the likely net benefit of each option?

Option One — Retain the status quo

Who would be affected

Businesses

158. Businesses would continue to have the option to notify when data breaches occur and utilise the OAIC Data Breach Guide.

Individuals

159. The notification of individuals whose personal information is the subject of a data breach will continue to occur if an APP entity voluntarily undertakes notification.

Government

160. Government agencies would continue to have the option to voluntarily notify individuals if there has been a breach of the individual's personal information. If agencies choose to notify individuals they would be able to use the OAIC Data Breach Guide to inform their approach.

161. The OAIC would continue to provide guidance for the management of data breaches in the Data Breach Guide and other related guidance material.

Net benefit analysis

162. Option One is unlikely to have any additional effect. Agencies and private sector organisations under the Privacy Act will continue to operate in accordance with the APPs, and be encouraged to continue to report significant data breaches to the OAIC and affected individuals. Public perceptions about responses to data breaches are likely to remain in favour of prompt reporting, which may drive the development of stronger security measures and increased compliance with the voluntary Data Breach Guide.

163. Under this option, there is likely to be little impact on the OAIC, who will continue to acquit its functions under the Privacy Act including in relation to providing guidance on data breaches. The ability of the Information Commissioner under section 33C of the Privacy Act to undertake assessments of APP entities relating to the APPs may see data breaches coming to light in addition to those breaches subject to voluntary notification. Furthermore, information about breaches is now regularly revealed when hackers publicly report on their efforts.

164. There will be little change for individual Australians, noting that they face existing risks without a mandatory scheme. There remains a possibility that they may continue not to be informed in the event that their personal information becomes compromised, thereby raising the risk they could suffer serious harm. As noted above, more undisclosed breaches may begin to come to light because of the Information Commissioner's powers, and the trend in hackers revealing their work. As also noted above, the OAIC's 2013 national privacy survey found that the large majority of Australians expected entities to be transparent about information security practices, and wished to be informed following loss of their personal information[55]. These kinds of customer preferences may encourage more entities to err on the side of reporting where there has been a breach.

165. There will be no additional impact on businesses subject to the Privacy Act and they will continue to be able to notify the OAIC of data breaches if they choose to do so. There will be no impact on small businesses as they are generally not subject to the Privacy Act. Larger not-for-profit organisations subject to the Privacy Act (because they have a turnover of greater than $3 million) will be in the same position as organisations that are subject.

Option Two - Introduce a mandatory notification of serious data breach scheme

Who would be affected?

Business

166. Businesses regulated by the Privacy Act would be required to notify the OAIC and affected individuals when personal information has been the subject of a data breach that a

[55] *Community Attitudes to Privacy Survey Research Report 2013*: OAIC.

reasonable person would conclude is likely to result in serious harm, unless an exception applies. Small businesses which are not subject to the Privacy Act will not be affected.

Individuals

167. Individuals would be affected by Option Two as they would be notified by entities when their personal information has been the subject of a data breach that a reasonable person would conclude is likely to result in serious harm.

Government

168. Government agencies regulated by the Privacy Act will be required to notify the regulator and affected individuals when personal information has been the subject of a data breach that a reasonable person would conclude is likely to result in serious harm unless the agency is subject to an exception. Exceptions would apply if notification would impact upon a law enforcement investigation or the operation of a secrecy provision in other legislation, if a data breach fell under existing notification requirements in the My Health Records Act, or if the regulator granted an exemption.

169. The introduction of the option will also affect the OAIC, as it will regulate Option Two.

Benefits

Businesses

170. Option Two would require mandatory notification following a data breach of personal information, credit reporting information, credit eligibility information or tax file number information — all of which are subject to existing security requirements in the Privacy Act — that a reasonable person would conclude is likely to result in serious harm to affected individuals.

171. Requiring notification may act as an incentive to the holders of the above information to adequately secure or dispose of that information. In other words, the adverse publicity occasioned by a notification may deter poor handling of such information, and increase the likelihood that adequate and reasonable measures are taken to secure it. This could thus be called the 'deterrent objective'. The ALRC viewed this as more of a secondary objective, although it has been part of the rationale for data breach notification laws in many other jurisdictions. A 2015 IT security and privacy survey identified increased regulation leading to improved data security as a developing trend[56]. Submissions to the 2015-16 consultation were divided on whether a notification requirement would support the 'deterrent objective'. Submissions from stakeholders including PwC and Electronic Frontiers Australia indicated Option Two would promote improved information security.

[56] *The Battle Continues: Working to Bridge the Data Security Chasm*, Protiviti, 2015, 23.

172. However, some submissions did not agree that a mandatory data breach scheme will result in widespread improvements to data security, stating that organisations intending to improve information security will do so regardless, and organisations with no such intention are unlikely to change this as a result of new legislation.

173. The creation of mandatory laws would also create a more level playing field for organisations. The Victorian Privacy Commissioner noted in its submission to 2012 consultation that only ethical and compliance-conscious organisations are likely to voluntarily report. Mandatory notification would assist in reducing (and possibly eliminating) incentives for organisations to suppress or deliberately conceal data breaches.

174. In its submission to the 2015-16 consultation, the OAIC identified consistent reporting of data breaches by entities as a significant benefit. The OAIC stated that, under the current voluntary or self-regulatory model, entities that tell their customers about a data breach may suffer disproportionate reputational damage compared with entities that deal with data breaches internally.

175. The OAIC submission provided an example of a security vulnerability on a relatively widely used platform that resulted in the exposure of several Australian entities' customer records. Some entities notified affected customers and the OAIC, and experienced adverse media coverage. However, the OAIC anticipates that as the platform was widely used, other entities may have also experienced a breach but did not notify affected individuals or the OAIC, thereby avoiding media scrutiny. The OAIC concludes that a level playing field introduced by a mandatory notification scheme will ensure that entities with good notification practices are not unfairly disadvantaged.

176. As identified by the OAIC in their submission to the 2015-16 consultation, a mandatory notification scheme would provide entities with greater clarity about what breaches need to be notified and may assist entities with their response to data breaches.

177. The proposed scheme would clarify for entities what sort of data breach is a 'notifiable breach', and help entities assess whether they have experienced a 'notifiable breach'. A requirement to notify individuals of a data breach may also benefit entities, as proactive and timely notification of a notifiable data breach:

- allows the entity, rather than the media, to state what has happened and how the entity is managing the breach;
- helps the entity rebuild public trust;
- demonstrates publicly that the entity takes privacy seriously; and
- demonstrates that the entity is working to protect affected individuals from the harm that could result from the data breach.

178. A key outcome of a well-balanced privacy framework is the provision of a safer and more transparent environment for Australians to entrust their personal information to agencies and organisations. Greater assurance about the safety of personal information will

encourage consumers to more fully engage in e commerce, thereby boosting Australia's digital economy and benefitting businesses.

179. In its submission to the 2015-16 consultation the OAIC also identified further benefits where entities notify the OAIC of a breach. In such situations the OAIC could:

- give the entity guidance on responding to the data breach;
- assist the entity to determine whether the breach has been contained;
- meaningfully respond to community enquiries about the breach; and
- explain to individuals steps they may take to protect their personal information.

Individuals

180. Option Two would ensure that individuals whom a reasonable person would conclude are likely to be at risk of serious harm due to a data breach are notified of the incident, and receive recommendations about steps they should take in response. The individuals would then have an opportunity to take corrective action to change or otherwise 'resecure' the information. The ALRC considered that this could be referred to as the 'mitigation objective'. For example, this might allow an individual to change passwords where those passwords have been hacked, to cancel credit cards if details have been stolen, or to change telephone numbers where silent numbers have been revealed.

181. Support of the mitigation objective of a mandatory data breach notification scheme has been unanimous across the numerous consultations undertaken on the proposed introduction of a mandatory data breach notification scheme.

182. Submissions to the 2015-16 consultation agreed that being notified of a data breach would enable individuals to protect their interests and that a key objective of a mandatory data breach notification scheme is consumer protection. The OAIC stated a mandatory data breach notification scheme would allow individuals to take steps that may limit the risks that result when personal information is compromised and identified a number of steps notification would enable an individual to take to minimise the impact of a breach, such as:

- cancelling credit cards,
- changing online passwords, and
- monitoring their credit reports.

183. The mitigation objective is expected to raise confidence amongst consumers about the entities that they are dealing with, and the increased transparency will provide consumers with more information to make informed choices about whether to transact with particular entities.

Costs

Businesses

184. The introduction of a mandatory scheme for entities regulated by the Privacy Act raises the question of what new compliance costs will be. It is expected that the overall impact of the option would be low for the following reasons:

- research indicates notification costs amount to only 2.3% of the overall cost of a data breach[57];
- the Privacy Act has a small business exception that would exclude around 94% of Australian enterprises from the proposed scheme[58];
- the OAIC expects only 200 notifications in the first year of the proposed scheme's operation;
- 40% of voluntary notifications the OAIC currently receives are from government agencies and have no cost to businesses;
- the proposed scheme's relatively high notification threshold, and provisions to allow entities to self-assess whether notification is required, will mean fewer notifications are required than comparable schemes in other overseas jurisdictions; and
- a simple, streamlined scheme is proposed with the intention that entities who already participate in the OAIC's voluntary scheme will experience minimal change.

1. Administrative costs

185. In the 2013 targeted consultation and the 2015-16 consultation privacy and consumer advocates argued that the costs would be minimal. These respondents argued that the costs of preventing breaches are in any case generally lower than the costs of handling them once they have occurred; and that it is widely recognised that it is good business practice to proactively manage risks rather than to merely react when something goes wrong. Further, these groups argued that the costs are likely to be mostly one-off and should be considered a normal business overhead for any organisation handling personal information.

186. The 2013 targeted consultation and the 2015-16 consultation sought specific information in an attempt to quantify the regulatory burden of a mandatory data breach notification scheme. Stakeholders were asked what are the likely administrative costs (quantified if possible) to private sector organisations under a mandatory scheme for entities that have systems in place to notify under the voluntary OAIC Data Breach Guide, as well as those that do not. Respondents identified a number of administrative costs:

[57] Ponemon Report, page 3.

[58] Based on statistics AGD commissioned from the Australian Bureau of Statistics in 2013.

- costs linked to notification methods (e.g. mail, telephone, resourcing) so that the actual costs would be incurred by specific business units within an organisation. It was noted that greater flexibility in the notification requirements would assist in containing costs associated with communicating to customers;

- other costs could be in the time and effort in formalising the process (e.g. internal communications, directives, and process mapping);

- increased insurance costs, which would be a consequence of an increased perceived business risk;

- costs associated with the need to engage additional legal counsel.

187. The 2013 targeted and the 2015-16 consultation did not receive specific costs estimates. There was no common view among respondents about the likely amount of costs, with respondents providing a broad range of general cost estimates on this issue. For example, one industry group respondent to the 2013 targeted consultation commented that larger organisations have stated clearly that the requirements of mandatory notification would involve capital expenditure running into millions of dollars, and the costs would vary depending on the amount of data held by the entity. Another industry group respondent believed there would be 'significant capital costs'.

188. Whilst the views above may be salient for companies without a data breach policy, it is relevant to note that many companies already participate in the voluntary scheme and/or have a relevant policy. A recent report assessed over 100 leading Australian consumer brands against privacy best practices and found over two thirds have a data breach policy[59].

189. In the 2015-16 consultation, Telstra stated that establishing similar compliance programs is resource and time intensive, but can be implemented within existing frameworks by larger organisations. Telstra submitted that, unlike larger organisations, smaller organisations unable to implement reporting requirements into existing frameworks may incur substantive compliance costs from the introduction of a mandatory data breach notification scheme but these costs can be lowered by less complex legislative requirements.

190. The Notifiable Data Breaches Bill has responded to numerous submissions that well-drafted legislation will reduce the regulatory burden of Option Two. The numerous consultations conducted on Option Two have resulted in an iterative drafting process between the Attorney-General's Department and stakeholders. This design process means the Notifiable Data Breaches Bill removes unnecessary detail and procedural requirements, provides greater clarity about key terms, introduces more flexibility and reduces costs for entities. Furthermore, the proposed scheme will be largely based on the current voluntary scheme, meaning the cost of the proposed scheme will be minimal on entities participating in the current voluntary scheme.

2. Cost of notification of a data breach

[59] *Deloitte Australian Privacy Index 2016: Trust Without Borders*, Deloitte, page 13.

191. Notification costs will have two components: the costs of notifying the OAIC and the cost of notifying individuals. It is expected that the OAIC will issue guidance material that will help entities assess what constitutes a notifiable data breach, and how to comply with the proposed scheme's notification requirements.

192. Given the magnitude of some data breaches, particularly in an online environment, it is expected that the main costs of notification of a data breach will be the cost of notifying affected individuals. The increasing ubiquity of electronic communication using email, social media and web publishing will decrease notification costs when compared to the more traditional forms of communication such as mail and telephone. Whilst a small and decreasing percentage of notification may continue to be by mail and telephone, it is expected that the vast majority of notifications would occur electronically.

193. Also relevant to the cost of notification is that the option would include mechanisms to ensure that direct notification to affected individuals would not be required if it was unreasonable (for example, if the associated cost to the business would be excessive in all the circumstances). In these circumstances, the business would be able to notify the serious data breach via its website (if any) and any other reasonable methods (such as posts on the business's social media channels, if any, or a newspaper advertisement if appropriate). Particularly in the expected small percentage of situations where a business could only notify affected individuals directly via mail and telephone, these mechanisms would be expected to reduce the cost of compliance for business and prevent businesses from incurring unreasonable notification costs.

194. Research indicates notification costs amount to a small percentage of the overall cost of a data breach. The Ponemon Report found that the average total cost of data breach for an entity was $2.64 million. In contrast, the cost of notifying regulators and affected individuals of a data breach was $0.06 million or 2.3% of the total cost[60].

195. The projected amount of notifications under the option is relatively low. Based on the current voluntary scheme and statistics from other jurisdictions, in the first year of the proposed scheme's operation the OAIC expects to receive only 200 data breach notifications.

196. When assessing the impact of the proposed scheme on businesses it is relevant to note that around 40% of notifications under the current voluntary notification scheme are related to government agencies and have no impact on businesses. Furthermore, one in five notifications under the current voluntary scheme have involved only a single individual's personal information and roughly half of all notifications have involved less than 100 people.

197. The proposed scheme would only require notification when a reasonable person would conclude that an unauthorised access, unauthorised disclosure or loss is likely to result in serious harm to affected individuals. This threshold is based on the relevant recommendation of the ALRC report and is the same threshold is used in the OAIC's current voluntary scheme. This means that notification would not be required following a data breach where the risk of harm is unlikely, or the potential harm not serious. This will mean

[60] Ponemon Report, pages 1-3.

notification would be required less often compared to jurisdictions such as California and the European Union, and the impact on businesses would be decreased accordingly.

3. Cost to small businesses

198. The proposed scheme will only apply to around 6% of Australian businesses. The Privacy Act exempts small businesses (entities with an annual turnover of $3 million or less) from the operation of the Privacy Act. This exemption does not apply to some small businesses, including those that provide a health service, are a credit reporting body, or trade in personal information. The Attorney-General's Department commissioned statistical analysis from the Australian Bureau of Statistics that showed that in 2013 about 94% of entities on the ABS Business Register are below the $3 million threshold and are therefore not likely to be subject to the Privacy Act or the proposed scheme.

199. However, there are a number of small businesses in that category which are subject to the Privacy Act because of exceptions to the Act contained in provisions such as subsection 6D(4), e.g. they trade in personal information. In the 2013 targeted consultation process, it was argued that mandatory data breach notification would place a disproportionate cost on small businesses which are subject to the Privacy Act, particularly in the direct marketing industry, as they may not be in a position (unlike larger organisations) to absorb some of the costs internally.

200. Conversely, in a submission to the 2015-16 consultation the Australian Bankers Association observed that a mandatory data breach notification scheme may grant an unreasonable advantage to new entrants to an industry, such as new businesses and start-ups that have an annual turnover of less than $3 million per annum, as they are not required to comply with the notification obligation.

4. Cost to not-for-profit organisations

201. Larger not-for-profit organisations that are subject to the Privacy Act (because they have a turnover of greater than $3 million) will be in the same position as organisations that are subject to the Act.

5. Cost to particular industry groups

202. Respondents to the 2013 targeted consultation process had mixed views about whether particular industry sectors would incur disproportionate costs through a mandatory data breach notification scheme. Most believed there would be no industry sector impacted disproportionately, although others believed that there would be in the case of:

- small businesses and start-ups (see Item 3 above); and
- some members of the financial services sector, given that the coverage includes APP regulated entities, credit providers and tax file number recipients.

6. Competition costs

203. A possible negative impact for small business is that individuals may be more tempted to use larger private sector organisations in the knowledge that they are subject to mandatory requirements in the event of a data breach. In the 2013 targeted consultation stakeholders suggested that, in the US, bigger companies support data breach laws because smaller competitors cannot meet the compliance requirements and some cease doing business. The proposed amendments are unlikely to raise these issues as they do not change the small businesses exemption in the Privacy Act. In addition, individuals who are likely to prefer larger firms due to regulated privacy protections may have already made this choice due to the fact that the Privacy Act already applies to those firms.

204. Industry group respondents noted there could be some positive and negative impacts on competition as a result of a mandatory scheme. For example, customers may choose to 'vote with their feet' given the likely increased publicity around data breaches or lack of breaches, potentially impacting positively on competition. This is supported by the Ponemon finding that, following a data breach, 56% of the costs associated with a data breach were incurred through indirect costs including increased customer 'churn rate' (the percentage of customers abandoning a business)[61]. Ponemon also found (while acknowledging the small sample size) that post-data breach churn rate varied between industries, with the service and financial service industries experiencing a relatively higher churn rate and, as a result, also reporting a higher per capita cost per breach[62].

205. In the 2013 targeted consultation another industry group noted that both general and specific competition issues would arise in the marketing and advertising industry. That group commented that, in general, data-driven marketing and advertising will be less competitive than alternate channels and platforms (such as mass marketing and advertising in traditional broadcast mediums and in print), if the costs of mandatory data breach notification results in a considerable increase in the price of data-driven marketing campaigns. As a result, the group's view was that mandatory data breach notification scheme would affect the most innovative companies working in Australia's digital economy.

206. Industry groups also commented that there was the potential for serious and costly reputational damage if the Commissioner directed an entity to notify a general form of notification (e.g. publication in a newspaper) rather than a targeted notification. A general form would bring exposure to a wider range of the public, including those that are not affected by the data breach.

207. Option Two responds to this concern by providing that the Information Commissioner, whilst being able to make directions about the information provided to individuals by entities, would not be able to direct entities on the form of notification. Instead, an entity would have discretion to undertake 'general publication' where notifying each affected individual of the data breach would be impracticable, in which case the entity would be required to notify the breach via its website (if any), and to take 'reasonable steps' to publicise the notification. This could include publicising the notification via a newspaper

[61] Ponemon Report, page 14.

[62] Ponemon Report, page 11.

or online advertisement, a social media posting, or any other method that is reasonable in the context of the entity's operations and the circumstances of the data breach.

208. Finally, an additional competition issue identified was the creation of a higher cost of entry to market. These businesses would be in a similar state to start-up entities, and, if subject to the Privacy Act, would need to factor in the costs associated with a mandatory data breach notification scheme. However, it is arguable that these costs are likely to be minor compared with other privacy obligations that will need to be adhered to once a new business starts and becomes subject to the Privacy Act.

Individuals

209. There is the possibility that, as a result of the introduction of a mandatory scheme, some entities may need to make internal changes to improve compliance with the Privacy Act and these costs may be passed on to consumers, thereby making transactions more costly.

Government

210. There is likely to be an impact on the OAIC. As the regulator, the OAIC will be expected to receive a larger number of notifications, and will have additional powers to utilise in the event that a failure to comply with a data breach obligation requires investigation. The OAIC also expects to receive a higher number of privacy complaints due to complaints from individuals who receive data breach notifications, and that it will also be necessary to use other regulatory powers in some cases (for example, to investigate data breach notifications that suggest an entity has systemic privacy compliance issues). It is expected OAIC will issue new guidance on the new provisions and will have increased requests from entities that are keen to ensure they comply with the new legislative requirements.

Cost of Option Two

211. **Table 2** calculates the cost to business entities subject to the Privacy Act of the introduction of a mandatory data breach notification scheme per annum. The figure is drawn from the OAIC's estimate of the amount of notifications that would occur under the option multiplied by the cost of notifying regulators and affected individuals as reported in the Ponemon Report less factors not included in the Regulatory Measurement Burden Framework being:

- agency costs; and
- estimated costs of relevant notifications (those that would satisfy the threshold for the proposed scheme) under the current voluntary scheme.

212. Costings for the proposed scheme have been limited to notification costs as:

- the Ponemon Report amount is inclusive of costs for the 'determination of all regulatory requirements'[63];

- the 2013 targeted consultation and the 2015-16 consultation was unable to quantify administrative costs to entities; and

- other substantive and administrative costs associated with the proposed scheme would be absorbed into the costs entities incur for general Privacy Act.

213. This option will be offset by the PayPal Australia Pty Ltd exemption under section 248 of the *Anti-Money Laundering and Counter-terrorism Financing Act 2016*.

Table 2: Regulatory burden and cost offset estimate table for Option Two

Average annual regulatory costs (from business as usual)				
Changes in costs **($ million)**	Business	Community organisations	Individuals	Total change in costs
Total, by sector	$6.3	$0	$0	$6.3
Cost offset **($ million)**	Business	Community organisations	Individuals	Total, by source
Agency	$6.3	$0	$0	$6.3
Are all new costs offset? Yes				
Total (Change in costs – Cost offset) ($ million) = $0				

Key cost assumptions

214. The OAIC projects that if Option Two is implemented the scheme will receive 200 notifications in its first year of operation. This information is based on the OAIC's experience handling voluntary data breach notifications, and comparisons with similar overseas jurisdictions.

[63] Ponemon Report, page 12.

215. The Ponemon Report found that, on average, data breach notifications cost $0.06 million per data breach. The report was drawn from an analysis of 26 data breaches in Australia in 2016 with the average number of records breached being 19,663 records. The study calculates notification costs to include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up[64]. The costing assumes that this is the average of an entity's costs under Option Two.

216. The OAIC estimates that 34% of notifications are made by Australian Government agencies under the current voluntary data breach notification scheme. The costing assumes the figure would be similar to the proportion of notifications made by Government agencies under this option.

217. The OAIC has indicated that approximately 40% of the notifications made under the voluntary scheme would satisfy the threshold of Option Two. As the OAIC expects a mandatory scheme will see data breach notifications double, the costing assumes this would mean 20% of Option Two notifications would also have been made under the voluntary scheme and excludes them from the costing.

218. Option Two will have an impact on community organisations with an annual turnover of $3 million or more. In Table 1 this impact is captured in the total costs to businesses.

Net benefit analysis

219. Option Two, the introduction of a mandatory data breach notification scheme, would be likely to have a net benefit.

220. Whilst there will be a regulatory impact on organisations from a scheme that compels them to notify individuals when their personal information has been breached, this impact will be decreased by a number of factors including the high notification threshold of Option Two and its considerable replication of the OAIC voluntary data breach notification system. The regulatory impact of a mandatory data breach notification scheme will be likely to be offset by the benefits of individuals being able to mitigate against the threats associated with the breaching of their personal information, particularly the threat of identity theft and crime, as well as the wider benefits associated with an improvement to the personal information security practices of organisations and increased consumer confidence in the digital economy.

221. The 'mitigation objective' outlined above is the primary benefit to individuals from the introduction of a mandatory data breach notification scheme. The main cost to individuals would be organisations passing on the regulatory impact of a data breach notification scheme to individuals, for example through increased costs. Given data breach can lead to identity theft and crime, which can have high financial and personal costs, the benefit of a mandatory data breach notification scheme is considerable and would offset any costs to individuals.

[64] Ponemon Report, 1, 12.

222. The ‘deterrent objective’ outlined above is likely see an improvement in the information security practices of businesses. Option Two will create a level notification playing field for businesses, provide certainty about the types of data breaches businesses should notify, build consumer trust in businesses that notify proactively, enable businesses to control messaging around data breaches, demonstrate that compliant businesses take privacy seriously and increase consumer trust and engagement in the digital economy.

223. The growth of specific ‘cyber insurance’ products could also mean that the cost of data breach notifications will not be a burden borne directly by an increasing number of businesses with cyber security coverage. As the frequency and magnitude of data breaches increase insurers’ underwriting responses are adapting[65]. Cyber insurance exclusions are being added to general policies, protection is being provided in specific cyber security policies and the purchase of these policies, which can include coverage of the cost of privacy notifications, is increasing[66]. A 2015 global survey with more than 10,000 participants found 59% of respondents had purchased cybersecurity insurance. The survey projected that the cyber insurance market will increase from $2.5 billion this year to $7.5 billion in 2020[67]. The coverage of cyber insurance in Australia is increasing, with one leading broker of cyber insurance policies stating it had written 750 policies from January to August 2016, up from just three policies in total in 2013 with an expectation that this will increase should a mandatory data breach notification scheme be introduced[68].

224. There will be an impact on the OAIC, as the regulator of the Privacy Act, through an increase in the number of data breach notifications and subsequent privacy complaints, the increased use of its regulatory powers and the need to provide guidance on a new mandatory data breach notification scheme. However, as more entities improve privacy practices, and more information about preventing data breaches is available, there may be a longer term decline in the number of notifications reported to the OAIC and affected individuals. Similarly, while entities may be more cautious in the shorter term and report more instances to the OAIC, that may decline over time as they more fully understand their obligations.

Option Three — Encourage industry to develop industry codes

Who would be affected?

225. Private sector organisations and agencies under the Privacy Act could be encouraged to consider developing industry codes that provide a self-regulatory framework tailored to particular industry needs. Such codes would be developed under Part IIIB of the Privacy Act,

[65] *Insurance Banana Skins 2015: The CFSI Survey of the Risks Facing Insurers*, PWC, pages 16-17.

[66] *Recent Australia Privacy Incidents Compared to Rest of World: Insurance Response*, Lowenstein, Eric and Kevin Kalinich, Privacy Law Bulletin April 2015. *Cyber Insurance Research Paper*, Centre for Internet Safety, 2013, pages 7-8.

[67] *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016*, PwC, pages 15-16.

[68] *Hacks, attacks and outages cause surge in cyber insurance*, Australian Financial Review, 23 August 2016.

which allows for the Information Commissioner to approve and register enforceable codes which are developed by entities, on their own initiative or on request from the Commissioner, or by the Commissioner directly.

226. Part IIIB codes do not replace or override existing requirements in the APPs. Instead, a code clarifies how particular APPs are to be applied or complied with in a specific industry context. A code may also include obligations that go beyond the requirements of the APPs or the Privacy Act, such as a commitment to undertake data breach notification in specific circumstances.

Benefits

Businesses

227. There could be a number of benefits to a particular industry sector in developing an industry code. Firstly, an industry code could give entities a sense of active ownership of their privacy obligations. Secondly, a code may send a positive statement to the community that a particular entity or group of entities are mindful of the privacy concerns of individuals and are pro-active in protecting their privacy rights. A code may also change the culture of an entity or industry by raising awareness of privacy and introducing a compliance regime. It may serve as a guide to privacy regulation by providing entities with a single document that incorporates all its related legislative requirements and is written in a way that is applicable to a particular industry. Finally, it may provide clarity, certainty and satisfaction to consumers seeking redress by incorporating privacy complaint handling procedures in a code.

228. A code-based approach would allow government and industry sectors to examine more carefully how data breach incidents impact directly on their own particular sectors, and tailor a framework that takes into account existing reporting requirements and compliance issues. This would recognise the need for a flexible approach over a one-size-fits-all legislative approach that may be more a burden for particular industries.

229. A confidential submission to the 2015-16 consultation supported option three over option two on the basis that an industry sector generally containing smaller businesses should be able to develop reporting processes that are administratively efficient for that sector.

Individuals

230. The development of codes may raise the expectations of individuals that entities will increasingly improve their privacy practices and that complaint mechanisms will be available.

Costs

Businesses

231. Entities subject to the Privacy Act may support the opportunity to create their own code, although this would require those entities to set aside resources to meet with industry counterparts to develop a relevant code. For codes developed under Part IIIB of the Privacy

Act, the Code Guidelines noted that significant resources may need to be allocated to the development and maintenance of a code, including the following matters:

- establishing an administrative mechanism responsible for developing the code;
- scoping and drafting the code;
- seeking legal or professional advice;
- involving all stakeholders (including consumers) in an effective public consultation on the draft code;
- establishing and financing a code administrator to oversee the operation of the code, including reporting on the operation of the code and initiating regular reviews of the code; and
- maintaining information about the code on a website, including a list of the entities bound by the code, where relevant[69].

232. It is possible that the costs associated with the development of a code may outweigh the costs of complying with a mandatory data breach notification scheme, particularly if the new model is largely based on the existing voluntary model.

233. The Privacy Act regulates a wide variety of industries. The Australian and New Zealand Standard Industrial Classification (**ANZSIC**) contains 19 broad industry divisions. There are entities regulated by the Privacy Act in all 19 divisions with numbers ranging from a few hundred to over 10,000 depending on the category. Therefore, any attempt to provide code coverage similar to Option Two would require multiple codes across multiple industry sectors with what would appear to be a duplication of resources.

OAIC

234. The impact on the OAIC is likely to be moderate to high, depending on its level of involvement in developing and approving each code. As the regulator, it will be expected to promote greater awareness of the OAIC Data Breach Guide and would be likely to receive an increase in requests from industry bodies seeking assistance in developing a code. If industry codes are successful in encouraging entities to improve privacy and information security practices, there may be a longer term decline in the number of data breaches entities experience, which would result in fewer notifications reported to the OAIC and affected individuals.

Cost for Option Three

[69] Code Guidelines, pages 4–5.

Table 3 calculates the cost to business entities of the creation of industry specific codes for data breach notifications and the cost of subsequent notifications. The costing includes the estimated cost of code development and the cost of notification under the codes.

This option will be offset by the following measures:

- PayPal Australia Pty Ltd exemption under section 248 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2016.
- HCL Australia Services Pty Ltd exemption under section 248 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2016.
- Telstra Corporation Ltd exemption under section 248 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2016.
- Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulation 2016.
- Statute Update Bill 2016.

Table 3: Regulatory burden and cost offset estimate table for Option 3

Average annual regulatory costs (from business as usual)				
Changes in costs **($ million)**	Business	Community organisations	Individuals	Total change in costs
Total, by sector	$8.2	$0	$0	$8.2
Cost offset **($ million)**	Business	Community organisations	Individuals	Total, by source
Agency	$8.2	$0	$0	$8.2
Are all new costs offset? Yes				
Total (Change in costs – Cost offset) ($ million) = $0				

Key cost assumptions

235. Based on stakeholder consultation, the costing assumes the cost of developing and administering an industry code to be $1 million.

236. The costing assumes the creation of 19 codes to cover-off all of the industry sectors in ANZSIC.

237. The costing assumes the cost of notification to businesses would be the same as those under Option Two.

238. Option Three will have an impact on community organisations with an annual turnover of $3 million or more. In Table 2 this impact is captured in the total costs to businesses.

Net benefit

239. If a Part IIIB of the Privacy Act code was developed, it would have to meet equivalent standards that are currently contained in the OAIC Data Breach Guide, otherwise it is unlikely to receive the Information Commissioner's approval. Given that the mandatory data breach notification scheme is largely based on the existing voluntary model, it is likely that many of the same costs issues identified under Option Two will be raised.

240. There is a risk is that there may not be a consensus among industry participants on a final draft code, which would leave personal information without important privacy protections. It is also unclear whether it would be feasible to develop industry codes which cover a significant proportion of the entities in each of the 19 individual ANZSIC sectors. In any case, the small amount of codes developed under the existing Privacy Act to date indicates that the code regulation framework is not a solution for all industry sectors.

241. Further, given the different range of industries regulated by the Privacy Act, and the different types of personal information being collected, this approach gives rise to the possibility of an inconsistent and fragmented approach being adopted. This raises the risk that a standardised approach to the handling of personal information will not be achieved, which would be generally inconsistent with the approach to privacy regulation. That may create confusion amongst consumers, who might be notified about a data breach that has occurred with a particular entity in one industry sector, but not another. Some entities may also be subject to more than one industry code (e.g. telecommunications providers) and may be required to implement different responses to data breaches that occur depending on which code is applicable.

242. The benefits of Option Three for individual Australians are uncertain, given the difficultly in predicting the number of codes likely to be developed, the quality of those codes, and the number of entities in each industry sector likely to be covered by those codes. Individuals' data breach notification experiences would most likely vary depending on the particular industry that experiences the breach and the nature and coverage of any data breach notification code applying to that industry. Although the OAIC's regulatory oversight and advisory role in a code-based approach might generate consumer confidence (to the extent consumers are aware of that role), unless codes are uniformly adopted across a range of

industry sectors, there remains a risk that individuals may continue to be kept unaware in the event that their personal information becomes compromised.

243. It would also be possible for industry to develop data breach notification codes outside of the process in Part IIIB of the Privacy Act. Such codes would have no bearing on entities' obligations under the Privacy Act, and the OAIC would have no direct regulatory oversight and advisory role over such codes. However, if non-Part IIIB codes are developed, individuals will have no guarantee that industries will develop codes that require notification in the event of a data breach, or at least require data breaches to be notified at the standard that would be introduced under Option Two. The different requirements that would apply across industry sectors would also be likely to raise confusion amongst the general public.

244. A non-standardised and inconsistent approach is also less likely to provide the necessary information to meet the 'informational objective', which is intended to provide better information to combat data breaches in the future.

Consultation

245. The Attorney-General's Department has undertaken extensive consultation of a mandatory data breach notification scheme:

2012 Consultation

246. On 19 October 2012, a Discussion Paper was released seeking public comments on whether Australia's privacy laws should include a mandatory data breach notification requirement and, if so, the possible elements of such a requirement.

247. The Government received 62 submissions in response to the issues paper. There were 24 submissions either strongly, or conditionally, in support of the introduction of a mandatory reporting scheme. There were 12 submitters who did not express a definitive view although most of these did not expressly oppose a mandatory scheme. The group supporting a mandatory scheme included Commonwealth and State privacy/information regulators, privacy and consumer advocates, academics, IT software and security companies, and some individuals.

248. There were 27 submitters that opposed a mandatory scheme on the grounds that the existing voluntary scheme is operating effectively, and that a mandatory scheme could bring additional compliance obligations. This group comprised private sector industry groups and individual companies in the banking, telecommunications, retail and online industries, and two key government agencies.

2013 targeted consultation

249. In April 2013, an Exposure Draft Privacy Alerts Bill was provided on a confidential basis to a targeted group of stakeholders. The purpose of the consultation was to obtain more information to assist the Government in making a decision about whether to introduce a mandatory data breach notification scheme.

250. The targeted group was invited to make any comments on the legislative model. It was also asked to make comments on how the legislative model would impact on the costs that regulated entities might incur as a result of a new legislative requirement.

251. The Government received nine submissions in response to the issues paper. These came from a range of industry groups representing banks, telecommunications providers, financial service providers, internet companies and direct marketers. Submissions were also received from privacy and consumer advocates.

2015–16 consultation

252. In response to the Government's commitment to introduce a mandatory data breach notification scheme, the Attorney-General's Department drafted the Serious Data Breaches Bill. The Serious Data Breaches Bill was based on the Privacy Alerts Bill with changes made to decrease the regulatory burden and further accommodate the feedback received during the 2012 consultation and the 2013 targeted consultation.

253. When it committed to introduce a mandatory data breach notification scheme, the Government also committed to consulting on the legislation. Accordingly, the Serious Data Breaches Bill was the subject of extensive consultation.

254. An exposure draft of the Serious Data Breaches Bill and a consultation draft of the Regulation Impact Statement (**RIS**) were published on the Attorney-General's website accompanied by a Discussion Paper. The RIS set out the general policy problem the Serious Data Breaches Bill sought to address, explained why the Serious Data Breaches Bill was the preferred solution to that problem, explored the expected regulatory impact, and sought to consult on general and specific regulatory matters.

255. Public submissions on the exposure draft of the Serious Data Breaches Bill and the RIS were sought for a 13 week period between 3 December 2015 and 4 March 2016. The Attorney-General issued a media release announcing the consultation, and the Attorney-General's Department announced the public consultation on its Facebook page and via its Twitter account. In addition to this public consultation the Attorney-General's Department contacted relevant businesses, civil society organisations and government agencies directly seeking submissions. Submissions on the consultation draft of the RIS were also sought on the Office of Best Practice Regulation's Best Practice Regulation website.

256. During the 13 week consultation period direct communication with relevant entities such as industry and advocacy groups were undertaken to assess the regulatory impact of the proposal. As with the public consultation, these stakeholders were provided with an exposure draft of the Serious Data Breaches Bill and the RIS to comment on. This direct consultation took the form of meetings and teleconferences with various industry and civil society stakeholders.

257. In addition to seeking general submissions on the RIS, the Department also sought specific information in an attempt to quantify the regulatory burden of a mandatory data breach notification scheme. To this end, stakeholders were invited to respond to the following questions:

1. What is likely to be the 'paper burden' or administrative costs (quantified if possible) to private sector organisations under the mandatory scheme in the Serious Data Breaches Bill? In particular, what will be the burden to ensure compliance with the mandatory scheme for entities that:

    i. have existing systems in place to make notifications (where necessary) consistent with the existing Data Breach Guide; and

    ii. have no existing data breach notification systems in place?

    What will be the ongoing compliance burden?

2. What form of communication would organisations foresee utilising to notify affected individuals of a serious data breach?

3. How can a mandatory data breach notification scheme be implemented in a cost effective manner?

258. The 2015-16 consultation received 56 written submissions from businesses, industry groups, individuals, academics, privacy advocates and government agencies and the Attorney-General's Department consulted with numerous stakeholders in meetings held in Sydney and Melbourne. In addition, the Attorney-General's Department offered all of those who provided written submissions with the opportunity to discuss their written submissions. The full and open consultation undertaken by the Attorney-General's Department is best practice and was identified as the optimal way of obtaining an understanding of the regulatory impact of the proposal as well as encouraging openness and trust in the process.

259. The 2015-16 consultation garnered widespread support for Option Two, the proposal to introduce mandatory data breach notification reporting. Of the 56 submissions received 38 strongly or conditionally supported the proposed mandatory reporting scheme. These submissions were received from a wide range of sources including businesses from varied industry sectors, industry bodies, civil society groups, individuals, academia, regulators and government agencies. There were 12 submitters who didn't express a definitive view although most of these did not expressly oppose a mandatory scheme. The majority of these were from industry groups. Six submissions opposed the proposed mandatory reporting scheme. Of these six, three were from digital marketing and games/entertainment businesses, two were from the health industry and one from the insurance industry.

260. Submissions to the 2015-16 consultation provided valuable feedback on the proposed provisions of the Serious Data Breaches Bill. The consistent theme in submissions on the regulatory impact of the introduction of a mandatory reporting scheme was that this impact would be lessened if identified issues including those above could be resolved and the scheme is as streamlined as possible. The Department has responded to this feedback, redrafted the Serious Data Breaches Bill as the Notifiable Data Breaches Bill, and made changes in order to improve the scheme and reduce its regulatory impact. In addition, a number of smaller changes have also been made to respond to submissions to the 2015-16 consultation.

261. Detailed discussion and analysis of the responses to the 2012 consultation, the 2013 targeted consultation and the 2015-16 consultation are outlined in the relevant sections of this RIS.

What is the best option of those considered?

262. In this RIS, three options have been considered:

- Option One: Maintaining the status quo; or
- Option Two: Introduce a mandatory data breach notification scheme.
- Option Three: Encourage industry to develop industry codes.

263. The best option is Option Two; the introduction of a mandatory data breach notification scheme. It would address concerns that under the status quo data breaches are being underreported and, given the link between data breaches and identity theft and crime, address the concerns that the underreporting of data breaches adds to the impact of identity theft and crime on individuals and the economy. Unlike Option One and Option Three it could provide certainty about what entities are subject to the requirement to notify, what data breaches should be the subject of notification, when notification should occur, who should be notified and how. It would have less regulatory impact than Option Three.

264. Option Two has been the subject of extensive consultation, including consultation on two iterations of an exposure draft Bill for a mandatory data breach notification scheme. Consultation submissions have informed the design of the Notifiable Data Breaches Bill that is proposed to implement Option Two. This extensive consultation will ensure the mandatory data breach notification scheme, if implemented, is as suitable as possible to addressing the issue of data breach and its associated risks and costs.

265. Option Two would require the introduction of a legislative requirement which would have impacts on businesses, individuals and the OAIC. Option Two would provide individuals with notification if a notifiable data breach of their personal information occurs. Concerns about the safety and security of personal information in the online environment have been identified as key issues for individuals (as evidenced in the findings of the OAIC's 2013 national privacy survey cited above). Notification would place individuals in a better position to take steps to mitigate against the possibility of identity theft or fraud, which might cause them financial loss. This will be an important measure to assist in combatting cybercrime and identity theft which have a considerable toll on the Australian economy, businesses and individuals.

266. Option Two is likely to improve business compliance with responsibilities under the APPs. Specifically, Option Two will likely see entities improving their information security practices in line with APP 11 and the requirement to protect the personal information the entity holds from misuse, interference and loss and from unauthorised access, modification and disclosure. Ponemon's analysis suggests that better information security practices would

help reduce the cost of data breaches. For example, extensive use of encryption reduced the average cost of data breach by $13.50 or 10% per breached record of information[70].

267. A mandatory notification scheme may also make entities focus on how long personal information needs to be retained. APP 11 requires organisations to destroy or permanently de-identify information that is no longer needed for the permitted purposes for which it may be used or disclosed. Improved compliance with this requirement may help avoid data breaches involving information that an entity no longer has any lawful purpose to retain: for example, of the Privacy Commissioner's 16 investigation reports about data breach incidents between 2011 and 2016, five involved failure to comply with the Privacy Act's destruction/de-identification requirements as they applied under the now-repealed National Privacy Principle 4 (requirements that have been replicated in the current APP 11.2).

268. A mandatory notification scheme may also result in improved compliance with rules relating to the collection of personal information. First, an entity is likely to more carefully consider what personal information it is necessary to collect. APP 3 requires private organisations to only collect personal information that is reasonably necessary for one or more of their functions or activities. As noted in the OAIC Data Breach Guide, personal information that is never collected cannot be mishandled[71].

269. Whilst the introduction of a mandatory data breach notification scheme may see businesses improving compliance with their obligations under the APPs, the cost of these improvements is not a burden being imposed by the scheme. Rather, any such costs are linked to compliance with extant obligations under the APPs and the Privacy Act that pre-date the introduction of the scheme.

270. As noted in the analysis, there will be cost impacts on businesses. The Privacy Act applies to private sector organisations that have a turnover of more than $3 million, and to some small businesses which are subject to the Privacy Act (e.g. those that trade in personal information). Whilst not quantified, a number of administrative costs have been identified by industry groups, such as creating notification methods, formalising internal processes and increased insurance and legal costs. To address some of these concerns, Option Two makes the means of notification more flexible.

271. Consultation feedback on the costs estimates of Option Two varied from a small group of stakeholders who believed there would be large costs amounts to most who believed there would be modest cost implications. Privacy and consumer advocates believed costs would be minimal, and should be considered necessary where an entity handled personal information. The Ponemon Report found the notification costs of data breaches is reducing[72].

[70] Ponemon Report, page 9.

[71] Data Breach Guide, page 8.

[72] Ponemon Report, page 12.

272. Whilst Option Two would have a regulatory impact on businesses, it would also have benefits. Option Two would provide consistent obligations on entities to report data breaches. This is in contrast to Option One and Option Three. Option One provides a voluntary system that has been identified as causing disproportionate reputational damage to entities that voluntarily notify data breaches as opposed to those that deal with breaches internally. Option Three would complicate rather than simplify notification requirements by creating multiple industry codes, with entities possibly being subject to multiple codes. In contrast Option Two will provide clarity around an entities' obligations to notify through legislation and guidance in a way that is absent under Option One and not possible under Option Three.

273. As identified by the OAIC in its submission to the 2015-16 consultation, Option Two will contribute to a well-balanced privacy framework, provide a safer and more transparent environment for Australians to entrust their personal information to agencies and organisations, encourage consumers to more fully engage in e commerce, and boost Australia's digital economy.

Implementation and evaluation

Amendment to the Privacy Act

274. Option Two would be implemented through amendment of the Privacy Act. The 2012 consultation, the 2013 targeted consultation and the 2015-16 consultation have provided the opportunity for stakeholders to comment on the scope of Option Two, as well as provide specific feedback on multiple iterations of draft amendments to the Privacy Act to implement Option Two. Feedback has been received from businesses, industry bodies, civil society, academia, individuals, regulators and agencies.

275. The 2013 targeted consultation provided feedback on the Privacy Alerts Bill. The Privacy Alerts Bill provided the basis of the Serious Data Breaches Bill which was the subject of the 2015-16 consultation. Feedback on the Serious Data Breaches Bill was used as the basis for the Notifiable Data Breaches Bill. It is expected that the Notifiable Data Breaches Bill will amend the Privacy Act to introduce Option Two. The Notifiable Data Breaches Bill has been designed in collaboration with those it will affect. This will ensure the Government will implement the most suitable mandatory data breach notification scheme.

Option Two based on current voluntary system

276. Importantly, the Notifiable Data Breaches Bill will implement a mandatory data breach notification scheme based in large part upon the voluntary system that currently operates. This will mean many agencies and organisations that participate in the voluntary system will have a minimal compliance burden. This fact, in tandem with the 12 month transition to commencement of Option Two, will reduce the impact of implementation on agencies and organisations.

12 month transition to commencement

277. Amendments to the Privacy Act to introduce Option Two would commence 12 months after the amendment receives Royal Assent. This will allow agencies and organisations a full year to transition to the commencement of a mandatory data breach notification scheme. This 'lead in time' before commencement will allow agencies and organisations to make necessary arrangements in advance of commencement and will reduce the immediate regulatory impact of Option Two.

278. The 12 month transition period to commencement was included in the exposure draft of the Serious Data Breaches Bill and was therefore subject to the 2015-16 consultation. Whilst some submissions to the 2015-16 consultation felt a mandatory data breach notification should commence as soon as possible, and others felt it should be further delayed, there was general support from agencies and businesses for a 12 month transition to commencement.

OAIC guidance

279. The OAIC has a number of guidance related functions regarding acts or practices that may have an impact on the privacy of individuals under section 28 of the Privacy Act, including the power to issue guidelines. In the lead up to commencement of the amendments to the Privacy Act to introduce Option Two, it would be expected that the OAIC will develop and publish guidance about the operation of the new scheme to assist agencies and organisations respond to the scheme and promote ease of compliance.

280. This guidance may be in the form of a modified Data Breach Guide, which underpins the current voluntary notification system. It is expected that the guidance material would provide guidance about the practical aspects of the scheme.

281. It would be expected that the OAIC will undertake consultation as necessary with stakeholders, including private sector organisations, in the development of that guidance material. A number of submissions from agencies and organisations to the 2015-16 consultation identified the importance of OAIC guidance material on a mandatory data breach notification scheme and the importance of OAIC consulting with stakeholders when developing this material.

Evaluation

282. It is expected that the OAIC will keep statistics on the operation on a mandatory data breach notification scheme. It is expected that such statistics could include the amount and severity of data breaches notified under the scheme as well as the type of industry that makes the data breach notification. These statistics are similar to those currently maintained by the OAIC for the voluntary data breach system. These statistics will assist evaluate a mandatory data breach notification system.

283. To review the effectiveness of the changes instituting Option Two it is proposed that these measures be reviewed 12 months after commencement. The review would include an assessment of the impact of the proposal and its effectiveness in meeting its objectives. The

review will be assisted by the statistics maintained by the OAIC discussed above and would include consultation with relevant stakeholders.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

Privacy Amendment (Notifiable Data Breaches) Bill 2016

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

Overview of the Bill

285. The Bill amends the *Privacy Act 1988* (**Privacy Act**) by inserting provisions imposing a data breach notification requirement on entities regulated by the Privacy Act (**entity**) in relation to eligible data breaches. The amendments will commence on a single day fixed by proclamation or 12 months from the day after the Bill receives Royal Assent.

286. 'Eligible data breach' is defined in the Bill. For the purposes of the Bill, an eligible data breach occurs where personal information held by an entity is subject to unauthorised access or unauthorised disclosure and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the personal information relates (**affected individuals**). A cyber intrusion involving the publication online of individuals' names and credit card numbers could be an example of an 'eligible data breach'. Another potential example could be the accidental publication of patient records by a medical practice. An eligible data breach would also occur where personal information is lost in circumstances likely to lead to unauthorised access or disclosure, where, assuming the access or disclosure occurred, a reasonable person would conclude that it would be likely to result in serious harm to affected individuals.

287. The Bill provides that, where an entity has suffered an eligible data breach, it must notify affected individuals as well as the Australian Information Commissioner, unless an exception applies. If practicable, entities must notify either:

- all individuals whose information was subject to unauthorised access, unauthorised disclosure or loss, or

- only those individuals who are deemed to be at risk of harm (noting that this group will also be notified under the first option).

288. If neither option is practicable, the entity must publish a notification on its website (if any) and take reasonable steps to publish the notification.

289. In addition, subject to some exceptions, the Commissioner may direct an entity to notify affected individuals of an eligible data breach. The notification requirements and available exceptions are largely the same in either case, with the notable difference that, when issuing a direction to notify, the Commissioner may require the entity to include in the notification specified information relating to the eligible data breach.

290. The Bill provides that an entity which fails to satisfy these notification requirements engages in an interference with the privacy of an individual. The Commissioner's existing powers to investigate, make determinations and provide remedies in relation to non-compliance with the Privacy Act may then apply.

291. The Bill's notification requirements are expected to result in more timely opportunities for individuals to promptly respond to an eligible data breach by changing passwords, cancelling credit cards or taking other action to avoid serious harm. It is also anticipated that the notification requirements will provide entities with an incentive to improve security standards relating to personal information.

Human rights implications

292. The Bill engages the following rights:

- the right to privacy—Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and
- the right to a fair trial—Article 14 of the ICCPR.

The right to privacy

293. Article 17 of the ICCPR provides that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

294. The Bill promotes the right to privacy in that it provides the protection of the law against unlawful interferences with privacy. Individuals who are notified of an eligible data breach will be able to take prompt measures to protect their privacy. Furthermore, the Bill creates an incentive for entities to improve security standards relating to personal information.

295. The Bill contains exceptions to the mandatory data breach notification provisions which limit the right to privacy as individuals will not be notified of an eligible data breach if one of these exceptions applies. This limitation of the right to privacy is permissible as each of these exceptions is reasonable, necessary and proportionate means to achieve the goals of this Bill and the Privacy Act as a whole.

<u>Remedial action exception</u>

296. The notification requirement will be limited where:

- an entity takes action following an unauthorised access or unauthorised disclosure of personal information, or a loss that leads to unauthorised access or unauthorised

disclosure, and that action that would lead a reasonable person to conclude that the access or disclosure would not be likely to result in serious harm to affected individuals, or

- an entity takes action following a loss of personal information with the result that unauthorised access or unauthorised disclosure of the information does not occur.

297. Importantly, this exception can only apply where an entity has taken action following unauthorised access, unauthorised disclosure or loss of information to ensure that harm to affected individuals cannot arise as a result of the access, disclosure or loss, as the case may be. Requiring notification in this scenario would not serve any harm mitigation purpose. This exception is therefore a reasonable, necessary and proportionate means to achieve the balance between the protection of privacy and the interests of entities to be able to resolve personal information security incidents on their own initiative wherever possible.

Exception for eligible data breaches of other entities

298. The notification requirement will be limited where an entity experiences an eligible data breach that is also an eligible data breach of one or more other entities, and one of these entities complies with the notification requirement. These exceptions will apply where more than one entity jointly and simultaneously holds the same particular record of personal information (for example, due to outsourcing, joint venture or shared services arrangements). The exceptions are designed so that, in these situations, only one of the entities which experienced the eligible data breach is required to notify the eligible data breach (it will be a matter for the entities concerned to decide which of the entities does so). This ensures that the Commissioner and affected individuals will receive a single notification of an eligible data breach in these situations, rather than requiring each entity to separately notify the Commissioner and affected individuals, which would potentially lead to confusion and 'notification fatigue' for individuals and increased costs for regulated entities. This exception is therefore a reasonable, necessary and proportionate means to achieve the balance between the protection of privacy and the compliance burden on regulated entities.

Law enforcement exception

299. The notification requirement will be limited where: (a) the entity is an enforcement body; and (b) the Chief Executive Office of the enforcement body believes on reasonable grounds that compliance with the notification requirement would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body. Where that is the case, the enforcement body must only notify the Commissioner (unless the Commissioner has given the enforcement body a direction to notify an eligible data breach, in which case the exception will not require the enforcement body to notify the Commissioner). A key objective of the Privacy Act is to balance the protection of privacy with the interests of entities in carrying out their lawful and legitimate functions and activities. Because of their role in providing security to the community, it would not be appropriate for the Bill to contain measures that could prejudice law enforcement activities. It is important to note that enforcement bodies will still have to comply with the notification requirement in circumstances where compliance would not prejudice an enforcement related activity. This

exception is therefore a reasonable, necessary and proportionate means to achieve the balance between the protection of privacy and the interests of enforcement bodies.

Commissioner's declaration exception

300. The notification requirement will not apply where the Commissioner decides, either on his or her own initiative or on application from the relevant entity, to issue a notice exempting the entity from complying with the requirement, either entirely or only for a particular period of time. For example, the exception could operate where notification would impede a law enforcement investigation or where the eligible data breach concerns matters of national security (and where the law enforcement exception is not available). The Commissioner will be required to only grant a notice in cases where the Commissioner is satisfied doing so is reasonable in the circumstances, having regard to the public interest, any relevant advice (if any) about the decision to grant a notice a law enforcement body or the Australian Signals Directorate gives to the Commissioner, or such other matters (if any) that the Commissioner considers relevant in the circumstances. These requirements ensure that the exception is only relied upon following consideration of whether the risks associated with notifying a particular eligible data breach would in all the circumstances outweigh the benefits of notification to affected individuals. This exception is therefore a reasonable, necessary and proportionate means to achieve the balance between the protection of privacy and the protection of the public interest.

Secrecy provision exception

301. Where compliance with the notification requirement would to any extent be inconsistent with a provision in a law of the Commonwealth (other than the Privacy Act) that prohibits or regulates the use or disclosure of information, the notification requirement will be limited to the extent of the inconsistency. If a secrecy provision has been prescribed in regulations under the Privacy Act, and compliance with the notification requirement would to any extent be inconsistent with the prescribed provision, then the notification requirement will not apply. This exception is necessary to ensure that the notification requirement does not inappropriately override secrecy provisions in other laws, again recognising that the Privacy Act balances the protection of privacy with the interests of entities in carrying out their lawful and legitimate functions and activities. Where the exception applies, and if the secrecy provision is not prescribed in the regulations, the entity will still be required to comply with the notification requirement to the extent that the provision in the other law allows, meaning that affected individuals may receive notification in some form. Secrecy provisions would only be prescribed in regulations after consideration of whether other exceptions in the Bill would be sufficient to avoid the harm that would be prevented through prescribing the secrecy provision. This exception is therefore a reasonable, necessary and proportionate means to achieve the objectives of the Bill and balance the protection of privacy with the interests of entities in carrying out their lawful and legitimate functions and activities.

eHealth record exception

302. The notification requirement where an access, disclosure or loss that would otherwise constitute an eligible data breach under the Bill has been, or is required to be, notified under

section 75 of the *My Health Records Act 2012* (**My Health Records Act**). Section 75 of the My Health Records Act establishes mandatory data breach notification requirements that apply to data breaches involving eHealth records, or the integrity of the broader eHealth system. This exception is intended to prevent situations where notification of a eligible data breach would be required under both the Bill and the My Health Records Act. Importantly, where the exception applies, the entity would still be required to comply with the notification requirement in section 75 of the My Health Records Act, which will ensure adequate consideration of the privacy of affected individuals. This exception is therefore a reasonable, necessary and proportionate means to ensure consistency between the Bill and the My Health Records Act.

The right to a fair trial

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

304. The Bill provides that an entity which fails to notify affected individuals of an eligible data breach engages in an interference with the privacy of an individual. This is a reasonable and proportionate provision because failure to notify can have similarly adverse consequences for individuals to other interferences with privacy, such as breaching an Australian Privacy Principle. A range of acts and omissions may constitute a breach of an Australian Privacy Principle, from disclosing personal information for the purposes of direct marketing to not properly notifying individuals that their personal information has been collected. Interferences with the privacy of an individual may attract a civil penalty where there has been a serious or repeated interference with the privacy of an individual.

305. The penalties that may be imposed are compatible with Article 14 of the ICCPR because the Privacy Act provides that all persons are equal before the courts and have a right to a fair and public hearing before a competent, independent and impartial court. A civil penalty can only be issued by the Federal Court or Federal Magistrates Court/Federal Circuit Court of Australia following an application by the Commissioner. No minimum penalty is prescribed. 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. The Privacy Act's civil penalty provisions incorporate appropriate safeguards, including the stipulation that in determining pecuniary penalties a court must take all relevant matters into account, including the circumstances of the contravention, the nature and extent of any loss or damage suffered because of the contravention and whether the entity has previously been found to have engaged in similar conduct. The Privacy Act also provides that an entity will not be liable for more than one pecuniary penalty in relation to the same conduct, and that a civil penalty order cannot be made if an entity has already been convicted of an offence involving the same conduct, or conduct that is substantially the same. These

provisions ensure that pecuniary penalties are proportionate to any contravention of a civil penalty provision, and protect the rights expressed in Article 14.

Conclusion

306. The Bill is compatible with human rights because it promotes the right to a fair trial in Article 14 and the right to privacy in Article 17 of the ICCPR, and to the extent that it may limit the right to privacy, those limitations are reasonable, necessary and proportionate to achieve the legitimate aims of the Bill and the Privacy Act.

NOTES ON CLAUSES

Preliminary

Clause 1—Short title

1. This clause provides for the short title of the Act to be the *Privacy Amendment (Notifiable Data Breaches) Act 2016*.

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 definitions of ‘at risk’ and ‘eligible data breach’ into existing subsection 6(1) of the Privacy Act. This item provides that the term ‘at risk’ has the meaning given by section 26WE, while ‘eligible data breach’ has the meaning given by Division 2 of Part IIIC, both of which are inserted into the Privacy Act by this Bill (see Item 3 below).

7. The definition of ‘at risk’ is relevant when determining which individuals are notified when an entity makes a notification under subsection 26WL(2) or 26WR(2) (see Item 3 below). The definition of ‘eligible data breach’ 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 existing subsection 13(4). New subsection 13(4A) is titled 'Notification of eligible data breaches etc.', and provides that if an entity (within the meaning of Part IIIC) contravenes either new subsection 26WH(2), 26WK(2), 26WL(3) or 26WR(10) of the Privacy Act (all of which are inserted by this Bill), the contravention is taken to be an act that is an 'interference with the privacy of an individual'. Existing 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 subsection 26WH(2), 26WK(2), 26WL(3) or 26WR(10), as the case may be. These include the capacity for the Commissioner to initiate investigations, make determinations and seek enforceable undertakings, as well as making applications for civil penalties for serious or repeated interferences with the privacy of an individual.

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 existing 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 inserted into the Privacy Act by this Bill (see Item 3 below).

Item 3 After Part IIIB

Part IIIC—Notification of eligible data breaches

12. Item 3 of Schedule 1 inserts a new Part IIIC, titled 'Notification of eligible 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 three Divisions. Broadly, the first Division sets out a simplified outline of the Part and contains some provisions which influence the scope of the Part, the second Division sets out when an 'eligible data breach' will have occurred, and the third Division contains obligations for entities to notify eligible data breaches, subject to limited exceptions.

Division 1—Introduction

Section 26WA Simplified outline of this Part

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

Section 26WB Entity

15. 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 26WB provides that, for the purposes of Part IIIC, 'entity' also includes a person who is a file number recipient. This will ensure that file number recipients which could experience an 'eligible data breach' as defined in section 26WE below but are not an agency, an organisation or a small business operator will nonetheless still be subject to the notification requirement.

Section 26WC Deemed holding of information

16. This section provides that, where particular kinds of entities subject to Part IIIC have disclosed information subject to the Part to particular recipients, the Part applies as though the entity held the information.

Overseas recipients

17. Subsection 26WC(1), which is titled 'Overseas recipients', establishes the circumstances under which an Australian Privacy Principle ('**APP**') entity will retain accountability for an eligible data breach involving personal information even though that APP entity might not be otherwise responsible for the breach due to the fact that the personal information has been disclosed to an overseas recipient.

18. Subsection 26WC(1) 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 Part IIIC 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 Part IIIC apply, and the disclosing APP entity retains accountability under existing section 16C of the Privacy Act for that personal information, even if the eligible data breach occurred offshore.

Bodies or persons with no Australian link

19. Subsection 26WC(2), which is titled 'Bodies or persons with no Australian link', establishes the circumstances under which a credit provider will retain accountability for an 'eligible data breach' involving credit eligibility information that was disclosed to a body or person with no Australian link.

20. Subsection 26WC(2) provides that where:

- either:
    - a credit provider has disclosed, under existing paragraph 21G(3)(b) or 21G(3)(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 existing 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 Part IIIC 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 existing subsection 21S(1) of the Privacy Act in relation to the credit eligibility information. This means that the requirements of Part IIIC 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 existing 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.

21. This item also inserts a Note following subsection 26WC(2) and before section 26WD. The Note provides a cross-reference to existing section 21NA of the Privacy Act, about disclosures to certain persons and bodies that do not have an Australian link.

Section 26WD Exception—notification under the *My Health Records Act 2012*

22. The effect of this section is to avoid imposing a double notification requirement if an unauthorised access, unauthorised disclosure or loss of information that may constitute an eligible data breach as defined in Division 2 below has also been, or is also required to be, notified under the existing mandatory data breach notification scheme in section 75 of the *My Health Records Act 2012*. Specifically, the references to an 'unauthorised access', 'unauthorised disclosure' or 'loss' of information in paragraphs 26WD(a), 26WD(b) and 26WD(c) link to the definition of an eligible data breach in Division 2 below to ensure that such an access, disclosure or loss does not constitute an eligible data breach under Division 2.

Division 2—Eligible data breach

Section 26WE Eligible data breach

23. This section sets out the circumstances in which an 'eligible data breach' occurs. In short, the section provides that an eligible data breach occurs where:

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

- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or in the case of loss of information, assuming that unauthorised access or unauthorised disclosure were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

Scope

24. Subsection 26WE(1), which is titled 'Scope', sets out the kinds of entities and information which a data breach must involve to satisfy the definition of an 'eligible data breach'. Each kind of entity included in the subsection is already subject to the Privacy Act. The subsection also provides that an eligible data breach can only occur in relation to information that is subject to existing Privacy Act information security requirements. This also has the effect of preserving existing exemptions in Privacy Act that apply to particular acts and practices (for example, the exemptions for organisations in existing section 7B), meaning that an eligible data breach arising from such an act or practice will not fall under Part IIIC because it is not subject to existing Privacy Act information security requirements.

25. The references to existing Privacy Act information security requirements in subsection 26WE(1) do not mean that an entity has breached those requirements in the event of an eligible data breach. For example, an entity may comply with those requirements but nonetheless still experience an eligible data breach due to circumstances that were not reasonably foreseeable.

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

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

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

27. 'Personal information' is defined in existing 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.

28. Paragraph 26WE(1)(b) provides that section 26WE applies if:

- a credit reporting body holds credit reporting information relating to one or more individuals (subparagraph 26WE(1)(b)(i)), and

- the credit reporting body is required to comply with existing section 20Q of the Privacy Act in relation to the information (subparagraph 26WE(1)(b)(ii)).

29. '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.

30. Paragraph 26WE(1)(c) provides that section 26WE applies if:

- a credit provider holds credit eligibility information relating to one or more individuals (subparagraph 26WE(1)(c)(i)), and

- the credit provider is required to comply with existing subsection 21(S)(1) of the Privacy Act in relation to the credit reporting information (subparagraph 26WE(1)(c)(ii)).

31. '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 existing 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.

32. Paragraph 26WE(1)(d) provides that section 26WE applies if:

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

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

33. '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. Existing 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.

Eligible data breach

34. Subsection 26WE(2), which is titled 'Eligible data breach', establishes the circumstances that will constitute an 'eligible data breach' when information within scope of section 26WE is subject to unauthorised access, unauthorised disclosure or loss. 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.

35. Paragraph 26WE(2)(a) provides that an eligible data breach will occur in situations where:

- unauthorised access to or unauthorised disclosure of information of a kind referred to in new subsection 26WE(1) occurs (subparagraph 26WE(2)(a)(i)), and

- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates (subparagraph 26WE(2)(a)(ii)).

36. Paragraph 26WE(2)(b) provides that an eligible data breach will occur in situations where information of a kind referred to in subsection 26WE(1) is lost in circumstances where:

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

- the access or disclosure, assuming it were to occur, would lead a reasonable person to conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates (subparagraph 26WE(2)(b)(ii)).

37. The 'reasonable person' element of subparagraphs 26WE(2)(a)(ii) and 26WE(2)(b)(ii) ensure that an entity cannot be taken to breach Part IIIC if they fail to determine that an unauthorised access, unauthorised disclosure or loss is or would be likely to result in serious harm, if a reasonable person in their position would not have been able to do so based on information available to them, either directly or following reasonable inquiries. Other elements of the Bill also provide greater certainty about how entities are to determine whether an eligible data breach has occurred, including the 'relevant matters' requirement in section 26WG and the assessment requirement in section 26WH below, where an entity suspects but does not have reasonable grounds to believe that an eligible data breach has occurred.

38. In the context of subparagraphs 26WE(2)(a)(ii), the phrase 'likely' is intended to ensure that an eligible data breach only occurs if a reasonable person in the entity's position (rather than the individual to whom the information relates, or any other person) would conclude that serious harm would be more probable than not to occur to any individuals to whom information relates following unauthorised access to or unauthorised disclosure of that information.

39. In the context of subparagraph 26WE(2)(b)(i), the phrase 'likely' is intended to ensure that loss of information will only be considered an eligible data breach if it is more probable than not that the information will be subject to unauthorised access or unauthorised disclosure as a result. Examples of where unauthorised access or unauthorised disclosure would not be likely following loss of information might 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.

40. In the context of subparagraph 26WE(2)(b)(ii), the phrase 'likely' is intended to have an equivalent meaning to the use of that phrase in subparagraph 26WE(2)(a)(ii) above, following a loss of information that is likely to lead to unauthorised access or unauthorised disclosure, and assuming that such access or disclosure were to occur.

41. Part IIIC does not define what constitutes 'serious harm' for the purposes of subparagraphs 26WE(2)(a)(ii) and 26WE(2)(b)(ii). Potential forms of serious harm will vary depending on the circumstances of the individual or individuals concerned and the circumstances of the particular or assumed incident of unauthorised access or unauthorised disclosure. Potential harms, depending on the circumstances, could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation. Even where a reasonable person would consider that the access, disclosure or loss would be likely to result in harm, the reasonable person would also need to consider the harm to be 'serious' in order for an eligible data breach to have occurred under subsection 26WE(2).

42. Part IIIC is expected to predominantly require notification of eligible data breaches where a reasonable person would conclude that there is a likely risk of serious financial, economic or physical harm to individuals. However, the likelihood of other kinds of serious harm (such as serious emotional or psychological harm, or serious harm to reputation) cannot be ruled out, especially for eligible data breaches involving health information, other forms of 'sensitive information' as defined in section 6(1) of the Privacy Act, or other information that would be considered 'sensitive' according to the ordinary meaning of the term. The 'relevant matters' contained in section 26WG below also require consideration of particular matters which may assist in determining whether a reasonable person would conclude a particular unauthorised access or unauthorised disclosure (assumed or otherwise) would be likely to result in serious harm.

Section 26WF Exception—remedial action

43. This section deals with cases where an eligible data breach occurs but the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, which experienced the eligible data breach is able to take action so that a reasonable person would conclude that an unauthorised access, unauthorised disclosure, or loss, as the case may be, would not be likely to result in serious harm to any of the individuals to whom the information relates. A similar exception applies where an entity takes action that prevents unauthorised access or unauthorised disclosure from occurring following a loss of information. If the action remediates harm only to a particular individual or individuals from a larger cohort of individuals whose information was compromised in an eligible data breach, the section also provides that notification to those particular individuals is not required.

44. The section does not define what constitutes 'action' of this kind. What constitutes an action which satisfies an exception contained in the section will vary, but in general terms may include any action which remediates a risk of serious harm, or prevents unauthorised access to or unauthorised disclosure of information from occurring following an eligible data breach or potential eligible data breach. In the case of the exceptions contained in subsections 26WF(1), 26WF(2), 26WF(4) and 26WF(5), the question of whether an action satisfies the applicable exception must be considered from the perspective of a reasonable person.

Access to, or disclosure of, information

45. Subsection 26WF(1), titled 'Access to, or disclosure of, information' applies where an eligible data breach has occurred under subsection 26WE(2)(a), but the entity takes action before the relevant unauthorised access or unauthorised disclosure results in serious harm to any of the individuals to whom the information relates. Examples of potential action that might fall under this subsection could include:

- A financial institution which becomes aware that customer account details have been accessed by unauthorised parties, and freezes the affected accounts before any fraudulent transactions occur.

- An entity which becomes aware that it has mistakenly emailed the information of one individual to another individual, asks the second individual to delete the information

without using or disclosing it, and is confident that the second individual has complied with that request.

- An entity which becomes aware that an employee has accessed information without malicious intent but without authorisation, where the entity restricts the employees' access to the information and otherwise ensures that no further unauthorised access, use or disclosure of the information occurs, and continues to otherwise comply with the Privacy Act in relation to the information.

46. If, as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of the individuals to whom the information relates, paragraph 26WF(1)(e) provides that the eligible data breach is not, and is taken never to have been, an eligible data breach of the entity concerned. In considering whether a reasonable person would conclude that harm is not likely, regard must be had to the list of 'relevant matters' contained in section 26WG below.

47. The effect of paragraph 26WF(1)(f) in these circumstances is that the eligible data breach is also taken to have never been an eligible data breach of any other entity. This paragraph would apply where one or more other entities also jointly and simultaneously hold the same particular record of information compromised in the eligible data breach. Extending the exception to these entities, if any, ensures that the entities are not required to notify an eligible data breach where the relevant harm to individuals has already been adequately remediated.

48. Subsection 26WF(2) applies where an eligible data breach has occurred under subsection 26WE(2)(a), but the entity takes action before the relevant unauthorised access or unauthorised disclosure results in serious harm to particular individuals to whom the information relates. The subsection is expected to apply in similar circumstances to subsection 26WE(2)(a) above.

49. If, as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to a particular individual or particular individuals, notification to that particular individual or those particular individuals under Part IIIC is not required (though notification may still be required to any other individuals who a reasonable person would conclude are still at risk of serious harm).

50. Subsection 26WF(2) is intended to apply in circumstances where an eligible data breach occurs involving information relating to one or more individuals, and the entity is only able to remediate harm in relation to a subset of particular individuals.

Loss of information

51. Subsection 26WF(3), titled 'Loss of information', applies where an eligible data breach has occurred under subsection 26WE(2)(b), but the entity takes remedial action before the relevant loss of information results in unauthorised access to or unauthorised disclosure of the information. Examples of potential action that might fall under this subsection could include:

- An entity which takes action to recover hard copy information that an employee of the entity left in a taxi, and the driver assures the entity that he or she has not accessed or disclosed the information while it was in his or her care. An entity in this case, assuming they consider the driver's assurance to be credible, might conclude that the entity's action has prevented an unauthorised access or unauthorised disclosure from occurring.

- An entity which remotely erases the memory of a lost or stolen device before its content can be accessed without authorisation.

52. The effect of paragraph 26WF(3)(e) in these circumstances is that the loss is not, and is taken never to have been, an eligible data breach of the entity. Paragraph 26WF(3)(f) has the same effect as paragraph 26WF(1)(f) above in relation to eligible data breaches involving records of information jointly and simultaneously held by more than one entity.

53. Subsection 26WF(4) applies where an eligible data breach has occurred under subsection 26WE(2)(b), and the entity takes action after the relevant loss of information has led to unauthorised access or unauthorised disclosure, but before the unauthorised access or unauthorised disclosure has led to harm to any of the individuals to whom the information relates. Examples of potential actions that might apply under this subsection are the same as those listed as potential examples under subsection 26WF(1) above.

54. The effect of paragraph 26WF(3)(e) in these circumstances is that the loss is not, and is taken never to have been, an eligible data breach of the entity. Paragraph 26WF(4)(f) has the same effect as paragraphs 26WF(1)(f) and 26WF(3)(f) above in relation to eligible data breaches involving records of information jointly and simultaneously held by more than one entity.

55. Subsection 26WF(5) applies where an eligible data breach has occurred under subsection 26WE(2)(a), and the entity takes action after the relevant loss of information has led to unauthorised access or unauthorised disclosure, but before the unauthorised access or unauthorised disclosure has led to harm to particular individuals to whom the information relates.

56. If, as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to a particular individual or particular individuals, notification to that individual or those individuals under Part IIIC is not required.

57. Subsection 26WF(5) is intended to apply in similar circumstances to subsection 26WF(2) above.

Section 26WG Whether access or disclosure would be likely, or would not be likely, to result in serious harm—relevant matters

58. This section provides a non-exhaustive list of matters relevant to assessing the likelihood of serious harm for the purposes of the Division. The effect of paragraphs 26WG(a) and 26WG(b) is that regard must be had to the relevant matters listed in section 26WG when determining whether a reasonable person would conclude that an access

or disclosure would be likely (for the purposes of section 26WE(2) above) or would not be likely (for the purpose of subsections 26WF(1), 26WF(2), 26WF(4) and 26WF(5) above) to result in serious harm to any of individuals to whom the information relates.

59. The 'reasonable person' element of this section makes clear that regard is intended to be had to these matters by considering information that would be available to a reasonable person in their position, including following reasonable inquiries.

60. 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 reasonable person would reach the aforementioned conclusion, in other cases, it may be that a reasonable person would only reach that conclusion when regard is had to the relevant matters as a whole.

61. Most of the relevant matters listed in section 26WG are based on matters identified in the current OAIC *Data Breach Notification: A guide to handling personal information security breaches*, or matters identified in Australian Law Reform Commission (**ALRC**) Report 108, *For Your Information: Australian Privacy Law and Practice*.

62. 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 Part IIIC, or to introduce specific security guidelines relating to Part IIIC. This could include guidance material about the matters in section 26WG and the process of determining whether a reasonable person would conclude that an access or disclosure would be likely or would not be likely to result in serious harm for the purposes of new subsection 26WE(2), 26WF(1), 26WF(2), 26WF(4) or 26WF(5).

63. Paragraph 26WG(c) provides that the kind or kinds of information concerned in a data breach is a relevant matter under section 26WG. 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 likelihood 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 likelihood of harm than a single piece of information. However, in assessing whether a reasonable person would conclude that an access or disclosure would be likely or would not be likely to result in serious harm, it is relevant to consider whether a reasonable person might reach such a conclusion because of the likelihood that the information could be combined with other information.

64. 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 remediate 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.

65. Paragraph 26WG(d) provides that the sensitivity of the information is a relevant matter under section 26WG. 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 26WG(c) above, and it is expected that the matters under paragraphs 26WG(c) and 26WG(d) could be considered together.

66. 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.

67. Paragraph 26WG(e) provides that whether the information is protected by one or more security measures is a relevant matter under section 26WG. 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 26WE(1).

68. In relation to electronic information, considerations that may apply under paragraph 26WG(e) may be similar or identical to matters that may be relevant under paragraph 26WG(h) below. 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 an eligible data breach has occurred than consideration of the matter dealt with under paragraph 26WG(h).

69. Paragraph 26WG(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 under section 26WG. Returning to the example mentioned in relation to paragraph 26WG(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 section 26WG (in particular paragraph 26WG(g) below).

70. Paragraph 26WG(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 under section 26WG. For the purposes of paragraph 26WG(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 serious harm to the individual to whom the information relates (for example, a person against whom the individual has a restraining order).

71. An example might be if information falling under subsection 26WE(1) was exfiltrated from an entity's IT network in a cyber intrusion. Paragraph 26WG(g) is intended to require the entity to have regard to whether the information was likely to have been obtained, or

could likely be obtained, by individuals with the capability and motive to use the information to cause harm to affected individuals, and whether this would influence a reasonable person's conclusion about whether the access would be likely or would not be likely to result in serious harm to any of the individuals to whom the information relates. 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 without authorisation, and the information could as a result be accessed by a person with the capability and motive to cause harm to affected individuals (such as a person intending to use the information to commit identity theft for financial gain).

72. Paragraph 26WG(h) has the effect that under section 26WG entities must, in short, have regard to:

- the likelihood that a security technique or methodology designed to make information compromised in a data breach unintelligible or meaningless, such as encryption, could be circumvented by individuals with the intent of causing harm, and

- whether that circumvention may contribute to a reasonable person concluding that an access or disclosure would be likely or would not be likely to result in serious harm to any of the individuals to whom the information relates.

73. Subparagraph 26WG(h)(i) applies if a security technology or methodology was used in relation to the information. 'Security technology or methodology' is intended to be a technology neutral term that could apply to a range of technologies or methodologies designed to operate in the way described in subparagraph 26WG(h)(ii). As such, while encryption is expected to be the most common 'security technology or methodology' falling under subparagraph 26WG(h)(ii), the subparagraph could also apply to other technologies or methodologies. One possible example could be tokenisation, where the information to be protected is substituted with a token that is meaningless to unauthorised parties. The phrasing of subparagraph 26WG(h)(i) also means that the security technology or methodology does not need to have been used in relation to the information by the entity itself: it could, for example, have been used by some other entity, including another entity which simultaneously holds the information, such as a cloud storage provider.

74. Subparagraph 26WG(h)(ii) applies where the security technology or methodology referred to in subparagraph 26WG(h)(i) above was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information. The reference to the 'design' of the security technology or methodology reflects that the subparagraph is concerned with the intended operation of the security technology or methodology rather than its effectiveness, which is dealt with under subparagraphs 26WG(h)(iii) and (iv) below. The inclusion of both 'unintelligible' and 'meaningless' in subparagraph 26WG(h)(ii) is intended to recognise that, in some cases, information falling under paragraph 26WG(h) may be wholly unintelligible to unauthorised parties, for example, if the information is contained in an encrypted file. In other cases, the information may be intelligible to an unauthorised party, but not in a way that holds any meaning as personal information, credit reporting information, credit eligibility information or tax file number information: for example, in the case of tokenised information, if the

unauthorised party would be able to determine that the same token links different records in a file of information, but would not be able to link the token to a particular identified or reasonably identifiable individual.

75. Subparagraphs 26WG(h)(iii) and (iv), read as part of the paragraph as a whole, go to the likelihood of whether the person, or kinds of persons, who have obtained, or could obtain, the information, have, or are likely to have, the intent of causing harm to any of the individuals to whom the information compromised in a data breach relates.

76. Subparagraph 26WG(h)(iii) requires entities to consider the persons, or kinds of persons, who have obtained, or who could obtain, the information. The considerations falling under this subparagraph are likely to be similar, if not identical in some cases, to those falling under paragraph 26WG(g) above. Particularly if the information has been published online, the entity might need to consider the likelihood of the persons, or kinds of persons, who could obtain the information at the time of the access or disclosure or at a later time.

77. Subparagraph 26WG(h)(iv) requires entities to consider whether the persons, or kinds of persons, referred to in subparagraph 26WG(h)(iii) above, have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates. Again, the considerations falling under this subparagraph are likely to be similar or identical to those falling under paragraph 26WG(g) above. The inclusion of subparagraph 26WG(h)(iv) means that paragraph 24WG(h) does not require entities to have regard to the ability of entities with advanced knowledge or resources (such as large technology firms) to circumvent the technology or methodology, if those entities are not likely to do so with the intention of causing harm to any of the individuals to whom the information relates.

78. After considering the matters in subparagraphs 26WG(h)(i)–(iv), entities are required to have regard to the likelihood that the person or kind of person referred to in subparagraph 26WG(h)(iii), with the intention to cause harm referred to in subparagraph 26WG(h)(iv), has obtained, or is likely to have obtained, information or knowledge required to circumvent the security technology or methodology referred to in subparagraphs 26WG(h)(i) and 26WG(h)(ii).

79. The reference to ‘information or knowledge’ in paragraph 26WG(h) is intended to reflect the different means by which a security technology or methodology falling under paragraph 26WG(h) could be circumvented. For example, ‘information’ in this context (as indicated in the note following the section, discussed below) could include an encryption key that could be used to decrypt information that was subject to unauthorised access or unauthorised disclosure: if the encryption key was also accessed or disclosed, or was obtained at a later time, the entity may have a strong indication that the encryption could be circumvented.

80. The reference to ‘knowledge’ in paragraph 26WG(h) is intended to include knowledge about a particular kind of security technique or methodology that could be used to circumvent the technology or methodology, and that might be available at the time of the data breach or that might become available at a later time (noting that such a consideration would be subject to the ‘likelihood’ element of paragraph 26WG(h)). For example, entities may need to consider the likelihood that knowledge about how to circumvent a particular

encryption algorithm which is fit for purpose by current standards may become available in future as computing power and mathematical knowledge increase.

81. Where entities have regard to the likelihood of circumvention at a later time, it is intended that they should do so with the intent of determining whether a reasonable person would conclude that an access or disclosure would be likely or would not be likely to result in serious harm at that time to any of the individuals to whom the information relates. In this situation the 'remedial action' exceptions in section 26WF above may also be relevant if an entity takes action to remediate the risk of serious harm to individuals before the security technology or methodology is likely to have been circumvented (for example, by taking action to prevent harm from arising from an unauthorised disclosure of information that was encrypted using an algorithm that was out-dated or otherwise not fit for purpose, and could be circumvented in a relatively short period of time).

82. The 'reasonable person' element of section 26WG ensures that regard must be had to the matter in paragraph 26WG(h) (as with all other matters in section 26WG) from the perspective of how the matter would influence the conclusion of a reasonable person about whether an access or disclosure would be likely or would not be likely to result in serious harm to any of the individuals to whom the information relates. Paragraph 26WG(h) is intended to require regard to had to the paragraph based on the information that would be known to a reasonable person in the entity's position or available to such a person following reasonable inquiries, rather than reflecting an expectation that it will be possible to assess the matters covered in the paragraph with absolute certainty.

83. Paragraph 26WG(i) provides that the nature of the harm that may occur as a result of a data breach is a relevant matter under section 26WG.

84. Paragraph 26WG(j) provides that any other relevant matter is also a relevant matter under section 26WG. 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 that might fall under paragraph 26WG(j).

85. This item also inserts a Note following paragraph 26WG(j) and before Division 3—Notification of eligible data breaches below. The Note explains that, if the security technology or methodology mentioned in paragraph 26WG(h) is encryption, an encryption key is the an example of information required to circumvent the security technology or methodology (as discussed above).

Division 3—Notification of eligible data breaches

Subdivision A—Suspected eligible data breaches

Section 26WH Assessment of suspected eligible data breach

86. This section sets out the circumstances in which an entity must carry out an assessment of whether an eligible data breach of the entity has occurred.

Scope

87. Subsection 26WH(1), which is titled 'Scope', provides that section 26WH applies where an entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity, but does not have reasonable grounds to believe that an eligible data breach of the entity has occurred. The intended relationship between section 26WH and section 26WK below is as follows:

- if an entity **is aware that there are reasonable grounds to suspect there may have been an eligible data breach of the entity**, but does not know if there are reasonable grounds to believe that there has been an eligible breach, the entity must carry out an assessment under section 26WH.

- if, on the other hand, an entity **is aware that there are reasonable grounds to believe there has been an eligible data breach of the entity** (after completing an assessment under section 26WH or otherwise), then the entity must prepare a statement under section 26WK.

88. This section is intended to apply where an entity becomes aware of circumstances that may constitute an eligible data breach, but needs to undertake a further assessment to determine whether an eligible data breach has occurred. For example, section 26WH might apply where a complaint from an individual leads an entity to suspect that there may have been an eligible data breach of the entity, but does not in itself provide sufficient information to give the entity reasonable grounds to believe that an eligible data breach has occurred.

89. Section 26WH is also intended 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 reasonable grounds to believe that an eligible data breach has occurred. Specifically, the reference to an entity that 'is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity' in subsection 26WH(1) is intended to make clear that entities are only required to carry out an assessment where some event or other circumstances has led the entity to become so aware.

90. 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.

91. The nature of an assessment under section 26WH will vary depending on the circumstances of the suspected eligible 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, and if so, whether this provides reasonable grounds to believe there has been an eligible data breach of the entity. On the other hand, if the entity has reasonable grounds to suspect 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 section 26WG above could assist entities in undertaking the assessment). Whether the entity has undertaken or could potentially undertake remedial action under section 26WF above may also influence the nature or scope of an assessment under section 26WH.

92. Where an entity fails to become aware that there are reasonable grounds to suspect there has been an eligible data breach of the entity, or fails to adequately undertake an assessment under new section 26WH, the Commissioner may be able to direct the entity to notify the serious data breach under section 26WR below.

93. The scope of section 26WH should be considered alongside existing APP 11.1 of the Privacy Act, which requires entities to take reasonable steps to secure personal information they hold from (among other things) unauthorised access, unauthorised disclosure and loss, all of which are included in the meaning of the term 'eligible data breach' as defined in Division 2. Existing section 20Q and subsection 21S(1) of the Privacy Act, as well as the current tax file number rules issued under existing section 17 of the Privacy Act, impose equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information respectively, and are all also mentioned in the definition of the term 'eligible data breach' in Division 2. Though an entity that fails to become aware that there are reasonable grounds to suspect an eligible data breach of the entity has occurred will not necessarily breach the applicable existing security requirement that applies to the information concerned, the various requirements for the entity to have taken 'reasonable steps' to secure personal information are expected to assist in placing entities in a position where they are able to become so aware where it would be reasonable for them to do so.

Assessment

94. Subsection 26WH(2), which is titled 'Assessment', provides in paragraph 26WH(2)(a) that, where subsection 26WH applies, the entity must carry out a reasonable and expeditious assessment of whether the relevant circumstances constitute an eligible data breach of the entity.

95. The reference to a 'reasonable and expeditious' assessment reflects an intention that an assessment should be limited to matters that are reasonably likely to be relevant in the circumstances, and should be conducted as promptly and efficiently as practicable in the circumstances. An assessment which considers a range of matters which could not reasonably be considered relevant in the circumstances, or that is not conducted as promptly or efficiently as possible in the circumstances, would not fall within the scope of paragraph 26WH(2)(a).

96. The phrase 'reasonable and expeditious' in paragraph 26WH(2)(a) is not intended to create a direct relationship in all circumstances between the time required to undertake a reasonable and expeditious assessment and the size of a potential eligible data breach (either in terms of the volume of information potentially involved, or the number of individuals potentially affected). For example, depending on the circumstances, the time taken to undertake a reasonable and expeditious assessment of an eligible data breach affecting a large number of individuals may take the same amount of time as an assessment of an eligible data breach affecting fewer individuals.

97. The phrase 'reasonable and expeditious' in paragraph 26WH(2)(a) is not intended to discourage entities from undertaking, or attempting to undertake, action to remediate the risk of harm under section 26WF above in favour of undertaking an assessment under section 26WH. It is intended that an 'expeditious' assessment could still occur where an

entity which suspects an eligible data breach has occurred takes time to undertake or attempt to undertake such remedial action, so long as they can justify their actions as 'expeditious' in all the circumstances should notification prove to be required following the assessment.

98. Paragraph 26WH(2)(b) provides that entities must take all reasonable steps to ensure that the reasonable and expeditious assessment referred to in paragraph 26WH(2)(a) is completed within 30 days after the entity becomes aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity. Paragraph 26WH(2)(b) reflects the view that 30 days is a preferable timeframe in which an assessment should be undertaken wherever possible, though importantly it does not require entities to complete an assessment within 30 days. Imposing a hard 30 day deadline to undertake assessments would not be appropriate, given that in the case of large or complex eligible data breaches 30 days may not be sufficient time to undertake a reasonable assessment. However, the intention of paragraph 26WH(2)(b) is to require entities to take all steps that are reasonable in the circumstances to attempt to complete the assessment within 30 days, so as to hasten notification to individuals if the assessment determines that an eligible data breach has occurred.

99. An entity which takes all reasonable steps to ensure that the assessment is completed within 30 days but is not able to complete the assessment in this time, for example because of the complexity of the suspected eligible data breach, will not be taken to have breached paragraph 26WH(2)(b). What constitutes 'all reasonable steps' in this context will vary depending on all the circumstances, including the circumstances of the entity and the suspected eligible data breach.

100. Regardless of the length of an assessment under subsection 26WH(2), the assessment (as per paragraph 26WH(1)(a)) must still be 'reasonable' in scope and completed within a timeframe that is 'expeditious' in the circumstances. This timeframe might be shorter or longer than 30 days depending on the circumstances.

101. This item also inserts a Note following subsection 26WH(2) and before section 26WK below. The Note explains that section 26WK applies where an entity has reasonable grounds to believe there has been an eligible data breach of the entity. This reflects that, in some cases, section 26WH will not apply in the event of an eligible data breach if it is clear to the relevant entity from the outset that the particular circumstances provide reasonable grounds to believe, as opposed to reasonable grounds to suspect, that there has been an eligible data breach of the entity.

Section 26WJ Exception—eligible data breaches of other entities

102. This section provides that:

- where one entity complies with new section 26WH above in relation to an eligible data breach (paragraph 26WJ(a)),

- and the applicable access, disclosure or loss, as the case may be, is also an eligible data breach of one or more other entities (paragraph 26WJ(b)),

- then section 26WH does not apply to that other entity or those other entities.

103. Section 26WJ is intended to apply in cases where more than one entity jointly and simultaneously holds the same particular record of personal information, for example, due to outsourcing, joint venture or shared services arrangements between entities. A specific example would be where an Australian Government agency stores personal information about employees in an electronic human resources system provided by another Australian Government agency, in circumstances where both agencies could be said to simultaneously 'hold' the personal information the first agency has stored in the system (according to the definition of 'hold' in existing subsection 6(1) of the Privacy Act).

104. The intended effect of section 26WJ is that only one assessment under section 26WH needs to be undertaken into a single eligible data breach, regardless of how many entities hold the record of information which was subject to unauthorised access, unauthorised disclosure or loss, as the case may be. Section 26WH is not intended to require each of the entities to separately undertake an assessment in this scenario. However, if none of the applicable entities undertakes such an assessment, each of the entities may be found to have breached section 26WJ, depending on the circumstances.

105. Section 26WJ is silent on which entity must complete the assessment under section 26WH where section 26WJ applies. The section does not, however, prevent the entity which undertakes the assessment under section 26WH above from making inquiries and seeking assistance from any of the other entities as required, or otherwise working with those entities, to complete the assessment.

Subdivision B—General notification obligations

Section 26WK Statement about eligible data breach

106. This section sets out the circumstances in which an entity must prepare a statement about an eligible data breach and provide that statement to the Commissioner.

Scope

107. Subsection 26WK(1), which is titled 'Scope', provides that section 26WK applies where an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity (as defined in Division 2 above). An entity might form such awareness following an assessment that is required to be undertaken under section 26WJ above or otherwise.

108. The inclusion of the phrase 'reasonable grounds' in subsection 26WK(1) should be read alongside the requirement in section 26WH above to undertake an assessment where the entity merely has reason to suspect that an eligible data breach of the entity has occurred. Subsection 26WK(1) is intended to ensure that notification is required both in cases where an entity is aware that an eligible data breach has occurred and where the evidence is not definitive but would nonetheless suggest (after an assessment has been completed under section 26WH or otherwise) that there are reasonable grounds to believe that an eligible data breach has occurred. What constitutes 'reasonable grounds' will vary depending on the

circumstances. For example, a pattern of complaints may provide the entity reasonable grounds to believe that an eligible data breach of the entity has occurred. On the other hand, if the complaints merely provide the entity with reason to suspect that there has been an eligible data breach of the entity, the assessment requirement under section 26WH will apply.

Statement

109. Subsection 26WK(2), which is titled 'Statement', provides that, where section 26WK applies, the entity must:

- prepare a statement that complies with subsection 26WK(3) (subparagraph 26WK(2)(a)(i)) (**a subparagraph 26WK(2)(a)(i) statement**)

- give a copy of the subparagraph 26WK(2)(a)(i) statement to the Commissioner (subparagraph 26WK(2)(a)(ii)), and

- do both of the above things as soon as practicable after the entity becomes aware that there are reasonable grounds to believe there has been an eligible data breach of the entity (paragraph 26WK(2)(b)).

110. The Commissioner may choose to publish guidance to assist entities to comply with the requirement to give a copy of the subparagraph 26WK(2)(a)(i) statement to the Commissioner. For example, the guidance material could ask entities to send a copy of the subparagraph 26WK(2)(a)(i) statement to a particular email address, or include details about additional information the Commissioner may ask entities to provide about an eligible data breach if the Commissioner considers that the information is required to undertake his or her functions under the Privacy Act.

111. What constitutes a 'practicable' timeframe for the purposes of paragraph 26WK(2)(b) to prepare a subparagraph 26WK(2)(a)(i) statement and give a copy of the statement to the Commissioner will vary depending on the time, effort or cost required to comply with paragraph 26WK(2)(b), when considered in all the circumstances of the entity and the data breach.

112. Subsection 26WK(3) outlines the information that must be set out in a subparagraph 26WK(2)(a)(i) statement. The required information is:

- the identity and contact details of the entity (paragraph 26WK(3)(a))

- a description of the eligible data breach that the entity has reasonable grounds to believe has happened (paragraph 26WK(3)(b))

- the kind or kinds of information concerned (paragraph 26WK(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 26WK(3)(d)).

113. The recommendations that must be included in the subparagraph 26WK(2)(a)(i) statement under paragraph 26WK(3)(d) are intended to provide individuals whose information has been compromised in an eligible data breach with general 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 an eligible data breach might result in credit fraud. While entities are expected to make reasonable efforts to identify and include recommendations that are relevant in the circumstances and would hold utility for individuals whose information was compromised in an eligible data breach, they are not expected to identify or include every possible recommendation that could be included following an eligible data breach. Guidance material from the Commissioner may assist entities in identifying the kinds of recommendations that entities could include under paragraph 26WK(3)(d).

114. The list of matters in subsection 26WK(3) that the subparagraph 26WK(2)(a)(i) statement must include does not prevent entities from providing individuals with other information about the eligible data breach in addition to the statement. For example, when providing the statement to affected individuals, entities might wish to additionally offer an apology to those individuals. Guidance material from the Commissioner may identify other kinds of information that entities may wish to consider including in addition to a subparagraph 26WK(2)(a)(i) statement.

115. The effect of subsection 26WK(4) is that, where an entity is preparing a subparagraph 26WK(2)(a)(i) statement for an eligible data breach which is also an eligible data breach of one or more other entities, the statement may also set out the identity and contact details of the other entities. This is intended to apply in cases where more than one entity jointly and simultaneously holds the same particular record of personal information, for example, due to outsourcing, joint venture or shared services arrangements between entities. Inclusion of this information is optional rather than mandatory to reflect that in some cases the information may not be of relevance to individuals receiving the notification. For example, if an individual has a customer relationship with the entity providing the subparagraph 26WK(2)(a)(i) statement, but is not likely to be aware of an outsourced service provider who also experienced an eligible data breach due to the same access, disclosure or loss, as the case may be, providing contact details for the latter entity may not serve any utility. Depending on the circumstances, it may be more appropriate to instead simply describe the outsourced service provider's role in the description of the eligible data breach under paragraph 26WK(3)(b) rather than providing the entity's contact details as per subsection 26WK(4).

Section 26WL Entity must notify eligible data breach

116. This section sets out how an entity must notify an eligible data breach after preparing a statement falling under section 26WK above.

Scope

117. Subsection 26WL(1), which is titled 'Scope', provides that section 26WL applies where an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity (paragraph 26WL(1)(a)), and the entity has prepared a

statement that complies with subsection 26WK(3) above (subparagraph 26WL(1)(b)(i)) and relates to the eligible data breach that the entity has reasonable grounds to believe has happened (subparagraph 26WL(1)(b)(ii)).

Notification

118. Subsection 26WL(2), which is titled 'Notification', sets out three possible options for notifying the subparagraph 26WK(2)(a)(i) statement. In short, an entity must either:

- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify each of the individuals to whom the relevant information compromised in an eligible data breach relates (paragraph 26WL(2)(a)), or

- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify those individuals who are considered to be 'at risk' from the eligible data breach, as defined in paragraph 26WE(2)(d) above (paragraph 26WL(2)(b)), or

- if it is not practicable to notify via either of the above two methods, notify the subparagraph 26WK(2)(a)(i) statement by publishing the statement on the entity's website (if any) (subparagraph 26WL(2)(c)(i)), and taking reasonable steps to publicise the statement (subparagraph 26WL(2)(c)(ii)).

119. These options are described in detail below. 'Practicability' in the context of paragraphs 26WL(2)(a)−(c) is intended to involve considerations about whether the time, effort or cost of a particular form of notification, when considered in all the circumstances of the entity and the data breach, would render such notification impracticable. Where an entity considers that it would not be practicable to comply with either paragraph 26WL(2)(a) or 26WL(2)(b), an entity must notify under paragraph 26WL(2)(c) (though other exceptions in Part IIIC may still apply, including an exception that applies because the entity applied to the Commissioner under section 26WQ below).

120. The concept of 'taking such steps as are reasonable in the circumstances' in paragraphs 26WL(2)(a) and 26WL(2)(b) is used elsewhere in the Privacy Act. As noted in the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 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.

121. Under paragraph 26WL(2)(a), if it is practicable to do so, an entity can take such steps as are reasonable in the circumstances to notify the contents of a subparagraph 26WK(2)(a)(i) statement to each of the individuals to whom the relevant information which has been or is assumed to have been subject to unauthorised access or unauthorised disclosure in an eligible data breach relates.

122. An entity might choose to notify a subparagraph 26WK(2)(a)(i) statement under this method, where it is practicable to do so, if it would require an unreasonable volume of resources for the entity to assess which affected individuals are 'at risk' from an eligible data breach and which are not. An example might be an eligible data breach involving

unauthorised access to a customer database containing varying amounts of personal information about a large number of individuals, where only some of those individuals might be 'at risk' due to the eligible data breach. Notification to the entire 'cohort' of individuals in this scenario may reduce the cost of compliance for the entity, and would also allow each individual who is notified of the contents of the subparagraph 26WK(2)(a)(i) statement to consider whether they need to take any action in response to the eligible data breach. It would also still ensure that all individuals who are 'at risk' receive notification.

123. Under subparagraph 26WL(2)(b), if it is practicable to do so, an entity can take such steps as are reasonable in the circumstances to notify the contents of a subparagraph 26WK(2)(a)(i) statement to those individuals who are 'at risk' from the eligible data breach.

124. An entity might choose to notify a subparagraph 26WK(2)(a)(i) statement under this method when the entity is able to ascertain with a high degree of confidence that only some particular individuals whose information has been or is assumed to have been subject to unauthorised access or unauthorised disclosure in an eligible data breach are 'at risk' from the eligible data breach. Returning to the customer database example above, if the entity was able to determine that the only likely result of serious harm from the eligible data breach would involve payment information stored in relation to a specific subset of the broader 'cohort' of individuals, meaning that only that subset is 'at risk' from the eligible data breach, the entity might choose to notify the contents of the paragraph 26WK(2)(a)(i) statement under paragraph 26WE(2)(b). As the entity could be confident that the remaining individuals would not be 'at risk' from the eligible data breach, notifying those individuals would serve no utility in the sense that they would not need to take any action to protect themselves from serious harm as a result of the eligible data breach.

125. In cases where all individuals whose information has been, or is assumed to have been, subject to unauthorised access or unauthorised disclosure in an eligible data breach are 'at risk' from the eligible data breach, there will be no practical difference between notifying the subparagraph 26WK(2)(a)(i) statement under paragraph 26WL(2)(a) or 26WL(2)(b).

126. Paragraph 26WL(2)(c) applies where neither paragraph 26WL(2)(a) nor 26WL(2)(b) applies — that is, where it is not practicable for an entity to notify the contents of a subparagraph 26WK(2)(a)(i) statement under either paragraph 26WL(2)(a) or 26WL(2)(b). In this situation, publishing a copy of the subparagraph 26WK(2)(a)(i) statement on the entity's website (if the entity has a website) is a suitable substitute notification method (subparagraph 26WL(2)(c)(i)), so long as the entity also takes reasonable steps to publicise the contents of the statement (subparagraph 26WK(2)(c)(ii)).

127. Subparagraph 26WL(2)(c)(i) does not prescribe precisely how entities must publish a statement on their website. It is intended that the statement will be published on the entity's website in a way that is reasonable in the circumstances.

128. The intended purpose of taking reasonable steps to publicise the contents of the subparagraph 26WK(2)(a)(i) statement under subparagraph 26WL(2)(c)(ii) is to increase the likelihood that the eligible 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 an eligible data breach to the attention of affected individuals. A simple step that would ordinarily be expected to be reasonable in the context of online publication would be ensuring that the subparagraph 26WK(2)(a)(i) statement can be indexed by online search engines. Other examples that may be reasonable depending on the circumstances include taking out a print or online advertisement in a publication or on a website the entity considers reasonably likely to reach affected individuals, or publishing an announcement on the entity's social media channels.

129. In some cases (such as an eligible data breach that involves a particularly serious form of 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 subparagraph 26WK(2)(a)(i) statement under subparagraph 26WL(2)(c)(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.

130. Possible approaches to publicising the contents of the subparagraph 26WK(2)(a)(i) statement as required under subparagraph 26WK(2)(c)(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 subparagraph 26WK(2)(a)(i) 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 26WL(2)(c)(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 26WL(2)(c)(ii), and the capabilities or requirements of the chosen channels vary.

131. Where an entity considers that compliance with paragraph 26WL(2)(a), 26WL(2)(b) or 26WL(2)(c) would not be reasonable in the circumstances, the entity may apply to the Commissioner for an exemption from the notification requirement (see section 26WQ below).

132. This item also inserts a Note following subsection 26WL(2) and before subsection 26WL(3) below. The Note directs readers to see also subsections 26WF(2) and 26WF(5), which deal with remedial action. As explained above, the effect of subsection 26WF(2) and 26WF(5) is that, if an eligible data breach occurs and the entity concerned is able to remediate the harm in relation to particular individuals among a group of individuals whose information was subject to unauthorised access, unauthorised disclosure or loss in the eligible data breach, the entity is not required to notify those particular individuals.

133. Subsection 26WL(3) provides that entities must comply with subsection 26WL(2) as soon as practicable after preparing the subparagraph 26WK(2)(a)(i) statement. Similar to

paragraphs 26WL(2)(a)–(c) above, 'practicability' in the context of subsection 26WL(3) is intended to capture considerations about whether the time, effort or cost of complying with subsection 26WL(2), when considered in all the circumstances of the entity and the data breach, would render such notification impracticable.

Method of providing the statement to an individual

134. Without limiting paragraph 26WL(2)(a) or 26WL(2)(b), subsection 26WL(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 26WL(2)(a) or 26WL(2)(b) 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, presented in ways they would expect from the relevant entity. 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.

Section 26WM Exception—eligible data breaches of other entities

135. This section provides that:

- where one entity complies with sections 26WK and 26WL above in relation to an eligible data breach (paragraph 26WM(a)),
- and the applicable access, disclosure or loss, as the case may be, is also an eligible data breach of one or more other entities (paragraph 26WM(b)),
- then sections 26WK or 26WL do not apply in relation to the eligible data breach of that other entity or those other entities.

136. This section is intended to apply in cases where more than one entity jointly and simultaneously holds the same particular record of personal information, for example, due to outsourcing, joint venture or shared services arrangements between entities. It is intended to work in the same way as other sections dealing with such scenarios, and in particular section 26WJ above, with the effect that only one subparagraph 26WK(2)(a)(i) statement must be prepared under section 26WK and notified under section 26WL for a single eligible data breach, regardless of how many entities hold the record of information that was compromised in the eligible data breach.

Section 26WN Exception—enforcement related activities

137. This section applies if:

- the relevant entity is an enforcement body (paragraph 26WN(a))

- the chief executive officer of the enforcement body believes on reasonable grounds that there has been an eligible data breach of the enforcement body (paragraph 26WN(b)), and

- the chief executive officer believes that compliance section 26WL would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, the enforcement body (paragraph 26WN(c)).

138. In these circumstances, paragraphs 26WK(3)(d) and section 26WL do not apply in relation to:

- the eligible data breach of the enforcement body (paragraph 26WN(d)), and

- if the eligible data breach was also an eligible data breach of one or more other entities — those entities (paragraph 26WN(e)).

139. 'Enforcement body' and 'enforcement related activities' are defined in existing subsection 6(1) of the Privacy Act. The effect of this provision is that an enforcement body is not required to notify affected individuals of the contents of the subparagraph 26WK(2)(a)(i) statement, either individually or in compliance with paragraph 26WL(2)(c) above. However, with the exception of paragraph 26WK(3)(d), the entity must still comply with subparagraphs 26WK(2)(a)(i) (i.e., the entity must prepare a statement that complies with paragraphs 26WK(3)(a), 26WK(3)(b) and 26WK(3)(c)) and subparagraph 26WK(2)(a)(ii) (i.e. the entity must give a copy of that statement to the Commissioner).

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

141. 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 eligible 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.

142. Paragraph 26WN(e) is intended to deal with similar circumstances to sections 26WJ and 26WM above, that is, where an enforcement body and one or more other entities (who may or may not also be enforcement bodies) jointly and simultaneously hold the same particular record of personal information that has been subject to an eligible data breach. Paragraph 26WN(e) ensures that the effect of this section is not undermined by requiring those other entities to notify the eligible data breach, where notification would prejudice one or more enforcement related activities undertaken by, or on behalf of, the enforcement body.

Section 26WP Exception—inconsistency with secrecy provisions

143. This section makes clear how the requirements in sections 26WK(2) and 26WL interact with secrecy provisions in other legislation. Different rules apply to particular secrecy provisions that have been prescribed in regulations under the Privacy Act for the purposes of this section.

Secrecy provisions

144. The effect of subsection 26WP(1), which is titled 'Secrecy provisions', is that for the purpose of this section a 'secrecy provision' is a provision of the law of the Commonwealth (other than the Privacy Act) that prohibits or regulates the use or disclosure of information.

145. Subsections 26WP(2) provides that, if compliance with the requirement in subparagraph 26WK(2)(a)(ii) to give the Commissioner a copy of a statement about an eligible data breach the entity has reasonable grounds to believe has happened would, to any extent, be inconsistent with a secrecy provision (other than a secrecy provision prescribed for the purposes of this section), subsection 26WK(2) does not apply to the entity to the extent of the inconsistency. (The reference to subsection 26WK(2) is intended to operate so that, where an entity is not required to provide a subparagraph 26WK(2)(a)(i) statement to the Commissioner because of subsection 26WP(2), the entity will not be required to nonetheless prepare such a statement under subparagraph 26WK(2)(a)(i).)

146. Subsection 26WP(3) applies in equivalent terms to subsection 26WP(2) in relation to the requirement under section 26WL to notify a subparagraph 26WK(2)(a)(i) statement to affected individuals.

147. In terms of assessing whether a secrecy provision is to 'any extent inconsistent' with subparagraph 26WK(2)(a)(ii) or section 26WL, subsections 26WP(2) and 26WP(3) are intended to operate so that:

- if a secrecy provision does not apply or otherwise does not prohibit a disclosure of information that is required or authorised by or under another law (such as subparagraph 26WK(2)(a)(ii) or section 26WL), inconsistency would not arise between the secrecy provision and subparagraph 26WK(2)(a)(ii) or section 26WL

- on the other hand, if a secrecy provision does apply, and does not provide an allowance for an entity to disclose information where required or authorised by or under another law, then inconsistency may arise between the secrecy provision and subparagraph 26WK(2)(a)(ii) or section 26WL, and

- if a secrecy provision provides a decision maker with discretion to disclose information or not, that discretion would remain in place (as a provision regulating the use or disclosure of information) in relation to the decision about whether to comply with subparagraph 26WK(2)(a)(ii) or section 26WL, so as to avoid inconsistency between subparagraph 26WK(2)(a)(ii) or section 26WL and the terms of the secrecy provision.

148. Subsections 26WP(2) and 26WP(3) also both require entities to comply with subparagraph 26WK(2)(a)(ii) or section 26WL except 'to the extent of the inconsistency' with a secrecy provision. This is intended to operate so that, if complying with those provisions in relation to only some of the information compromised in an eligible data breach would be inconsistent to any extent with a secrecy provision, the entity would still be required to comply in relation to any remaining information, if doing so would not be inconsistent to any extent with the secrecy provision in question (and if no other exceptions applied). In some cases it may also be possible for an entity to avoid inconsistency by complying with the notification requirements in a manner which does not disclose information that would give rise to inconsistency, for example, by preparing a subparagraph 26WK(2)(a)(i) statement which provides only very general information about an eligible data breach.

149. Another effect of subsections 26WP(2) and 26WP(3) is that entities can consider separately whether compliance would be inconsistent to any extent to the requirements contained in subparagraph 26WK(2)(a)(ii) and section 26WL. For example, it may be possible that notifying the Commissioner under subparagraph 26WK(2)(a)(ii) would not be inconsistent with a secrecy provision, but notifying individuals under section 26WL would be, in which case the entity would be required to notify only the Commissioner.

Prescribed secrecy provisions

150. Subsection 26WP(4), which is titled 'Prescribed secrecy provisions', provides that for the purposes of this section a 'prescribed secrecy provision' is a secrecy provision (as per the meaning in subsection 26WP(1)) prescribed in regulations under the Privacy Act.

151. The regulation-making power in subsection 26WP(4) will work in a similar way to the regulation-making power in existing paragraph 80P(7)(e) of the Privacy Act. The intention of including the regulation-making power is to ensure adequate flexibility in the event that it becomes apparent that it would be in the public interest for a new or existing secrecy provision in other Commonwealth legislation to prevail over the requirements contained in subparagraph 26WK(2)(a)(ii) or section 26WL, even if inconsistency would not otherwise exist between subparagraph 26WK(2)(a)(ii) or section 26WL and the prescribed secrecy provision. Consequently, the effect of subsection 26WP(5) is that a prescribed secrecy provision could be deemed to be inconsistent with subparagraph 26WK(2)(a)(ii) and section 26WL even if the prescribed secrecy provision allows an entity to disclose information where authorised or required by or under other laws.

152. Subsections 26WP(6) and 26WP(7) are intended to operate in a similar way to subsections 26WP(2) and 26WP(3) above. An important difference, however, is that subsections 26WP(6) and 26WP(7) lack the requirement that entities only need not comply 'to the extent of the inconsistency' between a secrecy provision and the requirements in subparagraph 26WK(2)(a)(ii) and section 26WL. This means that, if complying with subparagraph 26WK(2)(a)(ii) and section 26WL would to any extent be inconsistent with a prescribed secrecy provision, compliance is not required, even if compliance might have been required to some extent under subsections 26WP(2) and 26WP(3) if the secrecy provision had not been a prescribed secrecy provision.

153. It is intended that, before a secrecy provision is prescribed under this section, consideration would be given to whether existing exceptions in the new Part IIIC (such as the exception for enforcement related activities in section 26WN above, or the Commissioner's declaration power in section 26WQ below) are sufficient to avoid the kind of harm prescription in the regulations would be intended to avoid. It is also intended that consultation undertaken in accordance with section 17 of the *Legislation Act 2003* before prescribing a secrecy provision in regulations would include consultation with the Commissioner.

Section 26WQ Exception—declaration by Commissioner

154. This section provides that the Commissioner may, by written notice given to an entity, declare that the requirements to prepare a subparagraph 26WK(2)(a)(i) statement under section 26WK and notify that statement under section 26WL do not apply to the entity, or that the entity has until the end of specified period of time to comply with subsection 26WL(2) above (**a subsection 26WQ(1) declaration**).

155. The effect of paragraphs 26WQ(1)(a) and (b) is that the Commissioner can only give a subsection 26WQ(1) declaration to an entity where the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, or is informed by an entity that the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.

156. The effect of paragraph 26WQ(1)(b) is that an entity is only entitled to apply to the Commissioner under paragraph 26WQ(5)(b) below if the entity is aware that there are reasonable grounds to believe that an eligible data breach of the entity has occurred. This provision is intended to discourage entities from making an application if they do not have reasonable grounds to believe an eligible 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.

157. Where an entity is only aware that there are reasonable grounds to suspect there may have been an eligible data breach of the entity, the requirement to undertake an assessment of the relevant circumstances under section 26WH above will apply. If, after undertaking such an assessment, the entity forms the view that there are reasonable grounds to believe that an eligible data breach has occurred, the entity would be entitled to apply to the Commissioner under paragraph 26WQ(5)(b). Entities applying to the Commissioner under paragraph 26WQ(5)(b) would be required to do so as soon as practicable after the entity becomes aware of reasonable grounds to believe an eligible data breach of the entity has occurred. This is consistent with the notification timeframes in paragraph 26WK(2)(b) and subsection 26WL(3) above.

158. Where paragraph 26WQ(1)(a) or 26WQ(1)(b) apply, the Commissioner may give a subsection 26WQ(1) declaration to the entity stating:

- that sections 26WK and 26WL do not apply to the entity (subparagraph 26WQ(1)(c)(i)), or

- that the entity must comply with subsection 26WL(3), which requires entities to notify a subparagraph 26WK(2)(a)(i) statement under subsection 26WL(2) as soon as practicable after preparing that statement, as though subsection 26WL(3) instead required the entity to notify the statement under subsection 26WL(2) before the end of a period specified in the subsection 26WQ(1) declaration (paragraph 26WQ(1)(d)).

159. The effect of subparagraphs 26WQ(c)(ii) and 26WQ(d)(ii) is that, if the Commissioner gives a subsection 26WQ(1) declaration to an entity in relation to an eligible data breach that is also an eligible data breach of one or more other entities, the subsection 26WQ(1) declaration also applies to those entities. This is intended to operate in a similar way to sections 26WJ, 26WM and paragraph 26WN(e) above, in situations where one or more entities jointly and simultaneously hold the same particular record of personal information that has been subject to an eligible data breach. These subparagraphs should be read alongside subsection 26WQ(10) below, which deals with the ability of each entity in such a situation to apply to the Commissioner under paragraph 26WB(5)(b) separately in these circumstances. The subparagraphs should also be read alongside Item 4 and Item 5 below, which may provide review rights for each entity in some circumstances.

160. Subsection 26WQ(2) provides that a subsection 26WQ(1) declaration under paragraph 26WQ(1)(d) can only extend the period of time the entity has to comply with subsection 26WL(2) to the end of a period that the Commissioner is satisfied in reasonable in the circumstances. For example, if complying with subsection 26WL(2) would prejudice a law enforcement investigation into the circumstances of the eligible data breach (and the exception in section 26WN above would not apply), the Commissioner could give the entity a subsection 26WQ(1) declaration exempting the entity from complying with subsection 26WL(2) until a point in time when the Commissioner is reasonably satisfied that such prejudice will no longer occur.

161. Subsection 26WQ(3) provides that the Commissioner must not give an entity a subsection 26WQ(1) declaration unless the Commissioner is satisfied that it is reasonable in the circumstances to do so, having regard to:

- the public interest (paragraph 26WQ(3)(a))

- any ‘relevant advice’ given to the Commissioner by an enforcement body or the Australian Signals Directorate (**ASD**) of the Defence Department (subparagraphs 26WQ(3)(b)(i) and 26WQ(3)(b)(ii)), and

- such other matters (if any) as the Commissioner considers relevant (paragraph 26WQ(3)(c)).

162. For the purposes of subsection 26WQ(3), 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 giving a subsection 26WQ(1) declaration would be reasonable in the circumstances.

163. In terms of a mechanism to grant exemptions in the public interest, 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 include 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 ASD before applying to the Commissioner for a subsection 26WQ(1) declaration.

164. Advice is intended to be 'relevant advice' for the purposes of paragraph 26WQ(3)(b) when it is relevant to the Commissioner's decision to give a subsection 26WQ(1) declaration in relation to a particular eligible data breach. The 'relevant advice' could be given to the Commissioner either at the initiative of either an enforcement body or ASD, or on request from the Commissioner to those entities. It is also possible that an entity could provide a copy of such advice with appropriate bona fides when applying to the Commissioner for a subsection 26WQ(1) declaration under paragraph 26WQ(5)(b).

165. Subparagraph 26WQ(3)(b)(i) is intended to ensure that enforcement bodies can give advice about whether giving a subsection 26WQ(1) declaration to an entity is necessary to avoid prejudicing an enforcement related activity of the enforcement body (or another enforcement body). This subparagraph could apply to any entity included in the definition of 'enforcement body' in existing subsection 6(1) of the Privacy Act.

166. Subparagraph 26WQ(3)(b)(ii) applies to relevant advice from ASD because of ASD's cyber-security expertise and role in providing advice and assistance on information and communications security (including through the Australian Cyber Security Centre). For example, ASD might wish to give the Commissioner relevant advice that notifying an eligible data breach involving a cyber intrusion into an entity's IT systems before any relevant vulnerabilities have been addressed may result in further eligible data breaches of the entity, or raise other concerns.

167. The effect of subsection 26WQ(4) is that the 'relevant advice' provisions in paragraph 26WQ(3)(b) do not prevent the Commissioner from considering advice received or sought from other sources when deciding whether to give an entity a subsection 26WQ(1) declaration. The Commissioner could potentially consider advice of this kind under the requirement in paragraph 26WQ(3)(c) for the Commissioner to consider 'such other matters (if any) as the Commissioner considers relevant'. For example, if an entity applying for a declaration provided the Commissioner with a copy of advice about the eligible data breach received from CERT Australia — part of the Attorney-General's Department which provides assistance to Australian businesses about cyber security issues —the Commissioner would be required to consider such advice if he or she considered it relevant.

168. New subsection 26WQ(5) provides that the Commissioner may issue a subsection 26WQ(1) declaration either on the Commissioner's own initiative (paragraph 26WQ(5)(a)) or on application made by the entity (paragraph 26WQ(5)(b)). A decision by the Commissioner to refuse to give a subsection 26WQ(1) declaration on application by the entity, or a refusal to grant the entity the full extended period of time

requested by the entity to comply with subsection 26WL(2), will be reviewable by the Administrative Appeals Tribunal (see Item 4 and Item 5 below).

Applications

169. Subsection 26WQ(6), which is titled 'Applications', provides that an entity can apply to the Commissioner under paragraph 26WQ(5)(b) for:

- a paragraph 26WQ(1)(c) declaration: that is, a declaration that an entity does not need to comply with sections 26WK and 26WL in relation to an eligible data breach (paragraph 26WQ(6)(a))

- a paragraph 26WQ(1)(d) declaration: that is, a declaration that an entity has an extended period of time to notify an eligible data breach under section 26WL(2) (paragraph 26WQ(6)(b)), or

- a paragraph 26WQ(1)(c) declaration, or if the Commissioner is not disposed to make such a declaration, a paragraph 26WQ(1)(d) declaration: which is intended to recognise that in some cases where the Commissioner is not disposed to grant a paragraph 26WQ(1)(c) declaration, he or she may be willing to grant a paragraph 26WQ(1)(d) declaration, and should have discretion to do so in the interests of flexibility (paragraph 26WQ(6)(c)).

170. Subsection 26WQ(7) provides that, where the Commissioner refuses an application made by an entity under paragraph 26WQ(5)(b) for a subsection 26WQ(1) declaration, the Commissioner must give written notice of the refusal.

171. Subsection 26WQ(8) provides that:

- where an entity applies to the Commissioner for a paragraph 26WQ(1)(d) declaration nominating a particular specified time — that is, a declaration that the entity has until the end of the period of time the entity has nominated to comply with subsection 26WL(2) above, and

- the Commissioner decides to gives a paragraph 26WQ(1)(d) declaration for a different period of time

then the Commissioner's decision is taken not to be a refusal for the purposes of subsection 26WQ(7).

172. Subsection 26WQ(8) and Item 4 and Item 5 below together operate so that entities can nonetheless seek AAT review in the event that the Commissioner is willing to grant a subsection 26WQ(1) declaration, but not for the period of time for which the entity nominated in its application. Subsection 26WQ(8) is necessary for technical reasons to distinguish such a decision from a refusal by the Commissioner to grant a paragraph 26WQ(1)(d) declaration for any period of time, which is also a reviewable decision at the AAT under Item 4 and Item 5.

173. Subsection 26WQ(9) provides that, where an entity makes an application under paragraph 26WQ(5)(b) that, to any extent, relates to an eligible data breach of the entity, sections 26WK and 26WL above do not apply to:

- the eligible data breach (paragraph 26WQ(9)(a))
- if the access, disclosure or loss that constituted the eligible data breach is also an eligible data of one or more other entities—those other entities (paragraph 26WQ(9)(b))

until the Commissioner makes a decision on the application.

174. Subsection 26WQ(9) is intended to have similar effect to provisions in Part IIIC such as sections 26WJ, 26WM, paragraph 26WN(e) and in particular subparagraph 26WQ(1)(c)(ii) and subparagraph 26WQ(1)(d)(ii) above, in situations where one or more entities jointly and simultaneously hold the same particular record of personal information that has been subject to an eligible data breach. Subsection 26WQ(9) will ensure that, in these situations, where one entity applies to the Commissioner under paragraph 26WQ(5)(b), the timeframes for notification under sections 26WK and 26WL cease to apply to each of the entities until the Commissioner makes a decision on the application. This avoids complex compliance issues which could arise if the clock stopped for only some of the entities concerned, and is consistent with the provision in subparagraph 26WQ(1)(c)(ii) and subparagraph 26WQ(1)(d)(ii) that, in these situations, a subsection 26WQ(1) declaration applies to each of the entities concerned.

175. Subsection 26WQ(10) provides that an entity cannot apply to the Commissioner under paragraph 26WQ(5)(b) in relation to an eligible data breach where the access, disclosure or loss in question was also an eligible data breach of another entity that has already applied to the Commissioner under paragraph 26WQ(5)(b). This provision is included for efficiency reasons to ensure that the Commissioner does not receive multiple applications from different entities in relation to the same eligible data breach.

176. An entity who cannot apply to the Commissioner because of subsection 26WQ(10) will still be excused from complying with the timeframes for notification under sections 26WK and 26WL while the Commissioner makes a decision on the application (due to subsection 26WQ(9) above). If the Commissioner gives a subsection 26WQ(1) declaration in response to an application from one of the other entities who experienced the eligible data breach, an entity which could not apply to the Commissioner because of subsection 26WQ(10) will also be excused from complying with sections 26WK and 26WL in the same way as the entity which applied to the Commissioner. Finally, if the Commissioner refuses to give a subsection 26WQ(1) direction to an entity, another entity who was prohibited from applying to the Commissioner in relation to the same eligible data breach because of subsection 26WQ(10) may be able to seek review of the Commissioner's decision under Item 4 and Item 5 below.

Extension of specified period

177. Subsection 26WQ(11), which is titled 'Extension for specified period', can apply where the Commissioner has given a paragraph 26WQ(1)(d) declaration to the effect that an entity has until the end of a period of time nominated in the paragraph 26WQ(1)(d) declaration to comply with subsection 26WL(2) above. Subsection 26WQ(11) provides that the Commissioner can subsequently give the entity concerned a written notice extending the period of time specified in the declaration. The decision to grant such an extension will be at the Commissioner's discretion.

Subdivision C Commissioner may direct entity to notify eligible data breach

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

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

179. Subsection 26WR(1) provides that if the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible 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 subsection 26WR(4) below (paragraph 26WR(1)(a)) (**a paragraph 26WR(1)(a) statement**), and

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

180. Before giving a direction under subsection 26WR(1) **(a subsection 26WR(1) direction)**, the Commissioner must be aware that there are 'reasonable grounds' to believe that an eligible 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 become aware that there are reasonable grounds to believe that the entity has experienced an eligible data breach.

181. Subsection 26WR(2) provides that a subsection 26WR(1) direction must require entities to:

- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify each of the individuals to whom the relevant information compromised in an eligible data breach relates (paragraph 26WR(2)(a)), or

- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify those individuals who are considered to be 'at risk' from the eligible data breach, as defined in paragraph 26WE(2)(d) (paragraph 26WR(2)(b)), or

- if it is not practicable to notify via either of the above two methods, notify the paragraph 26WR(1)(a) statement by publishing the statement on the entity's website (if any) (subparagraph 26WR(2)(c)(i)), and taking reasonable steps to publicise the statement (subparagraph 26WR(2)(c)(ii)).

182. These requirements are based on actions that an entity must take when notifying a subparagraph 26WK(2)(a)(i) statement under subsection 26WL(2) above.

183. This item also inserts a Note following subsection 26WR(2) and before subsection 26WR(3) below. The Note directs readers to see also subsections 26WF(2) and 26WF(5), which deal with remedial action. As explained above, the effect of subsections 26WF(2) and 26WF(5) is that, if an eligible data breach occurs and the entity concerned is able to remediate the harm in relation to particular individuals among a group of individuals whose information was subject to unauthorised access, unauthorised disclosure or loss in the eligible data breach, the entity is not required to notify those particular individuals.

184. Subsection 26WR(3) provides that, before giving an entity a subsection 26WR(1) direction, the Commissioner must invite the entity to make a submission in relation to the direction the Commissioner is deciding whether to give under section 26WR within a period specified in the invitation (subsection 26WR(3)).

185. Subsection 26WR(3) is intended to ensure that entities have a right of reply before the Commissioner gives the entity a subsection 26WR(1) direction. For example, the entity might respond to the invitation by providing evidence to the Commissioner demonstrating that an eligible data breach has not occurred. On the other hand, an entity might decide to voluntarily notify the eligible data breach after receiving the Commissioner's invitation, rather than waiting for the Commissioner to give a subsection 26WR(1) direction. The form of the invitation, and the period of time specified in the invitation for the entity to respond, will be for the Commissioner to determine depending on the particular circumstances. In deciding the form and period of time to respond specified in an invitation, it is intended that the Commissioner would have regard to the impact on the entity and the nature and imminence of the risk of harm to individuals who would receive notification of the eligible data breach the Commissioner has reasonable grounds to believe has happened.

186. Subsection 26WR(4) sets out the contents of the paragraph 26WR(1)(a) statement that an entity must prepare to give notice of an eligible data breach. These are based on the matters that must be included when an entity has an obligation to prepare a subparagraph 26WK(2)(a)(i) statement (see subsection 26WK(3) above). The statement must include:

- the identity and contact details of the entity (paragraph 26WR(4)(a))

- a description of the serious data breach that the Commissioner has reasonable grounds to believe has happened (paragraph 26WR(4)(b))

- the kinds of information concerned (paragraph 26WR(4)(c)), and

- recommendations about the steps that individuals should take in response to the data breach that the Commissioner has reasonable grounds to believe has happened (paragraph 26WR(4)(d)).

187. Subsection 26WR(5) provides that the Commissioner, in issuing a subsection 26WR(1) direction, may also require that the paragraph 26WR(1)(a) statement set out specified information that relates to the eligible data breach that the Commissioner has reasonable grounds to believe 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 an eligible data breach on individuals is particularly high, such as if individuals are at increased risk due to the time that has elapsed since the eligible data breach occurred. The specified information that relates to an eligible data breach is intended to be information that the Commissioner considers would assist individuals to take appropriate action in response to the eligible data breach. Examples could include:

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

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

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

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

188. The Commissioner would not be required to specify additional information that must be set out in a paragraph 26WR(1)(a) statement under subsection 26WR(5). A decision by the Commissioner to require the inclusion of specified information relating to the eligible data breach in the paragraph 26WR(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 an eligible data breach (see new Item 4 and Item 5 below).

189. Subsection 26WR(6) sets out the matters to which the Commissioner must have regard before giving a section 26WR(1) direction, which are:

- any ‘relevant advice’ given to the Commissioner by an enforcement body (subparagraph 26WR(6)(a)(i) or ASD (subparagraph 26WR(6)(a)(ii))

- any ‘relevant submission’ made by an entity in response to an invitation under subsection 26WR(3) (subparagraph 26WR(6)(b)(i)), received by the Commissioner within the period specified in the invitation (subparagraph 26WR(6)(b)(ii)), and

- such other matters (if any) as the Commissioner considers relevant (paragraph 26WR(6)(c)).

190. These matters are based on the matters that the Commissioner must have regard to before giving a subsection 26WQ(1) declaration.

191. The effect of subsection 26WR(7) is that the 'relevant advice' provisions in paragraph 26WR(6)(a) do not prevent the Commissioner from considering advice received or sought from other sources when deciding whether to give an entity a subsection 26WR(1) direction. Subsection 26WQ(7) is based on the equivalent provision in subsection 26WQ(4) above.

192. Subsection 26WR(8) provides that, if the eligible data breach which is subject to a subsection 26WQ(1) direction is also an eligible data breach of one or more entities, the subsection 26WQ(1) direction may require the entity which receives the direction to include in the resulting subparagraph 26WR(1)(a) statement information about the identity and contact details of those other entities. This provision is based on subsection 26WK(4) above, which provides that entities can include such information when preparing a subparagraph 26WK(2)(a)(i) statement. In the same way as subsection 26WK(4) applies to entities, subsection 26WR(8) is an optional matter for the Commissioner to consider when giving a subsection 26WR(1) direction rather than a mandatory requirement, reflecting that the information may not hold utility to individuals receiving the notification in all cases.

Method of providing the statement to an individual

193. Without limiting paragraph 26WR(2)(a) or 26WR(2)(b), subsection 26WR(9), 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 26WR(2)(a) or 26WR(2)(b) may use that method. This provision is based on subsection 26WL(4) above.

Compliance with direction

194. Subsection 26WR(10), which is titled 'Compliance with direction', provides that an entity must comply with a subsection 26WR(1) direction as soon as practicable after the direction is given. This provision is intended to have the same effect as paragraph 26WK(2)(b) and subsection 26WL(3) above.

Section 26WS Exception—enforcement related activities

195. *S*ection 26WS, which is titled 'Exception—enforcement related activities', provides an exception for law enforcement bodies from complying with a subsection 26WR(1) direction in some circumstances. The exception is based on the exception that applies under subsections 26WN(a), 26WN(b) and 26WN(c) above where an enforcement body is not required to notify eligible data breaches in some circumstances.

196. The key difference between section 26WS and subsections 26WN(a), 26WN(b) and 26WN(c), however, is that the enforcement body does not have to provide notification to the Commissioner after the Commissioner gives the enforcement body a subsection 26WR(1) direction. This reflects an expectation that, where this exception applies, the circumstances of the eligible data breach will be such that there would be reasonable grounds to believe that

even notifying the Commissioner would prejudice an enforcement related activity conducted by or on behalf of the entity. However, it is expected that the Commissioner may in any case have some awareness of the details of the eligible data breach in question if the enforcement body provides a submission to the Commissioner under subsection 26WR(3) before the Commissioner gives the enforcement body a subsection 26WR(1) direction.

197. It is also expected that, where the Commissioner intends to issue a subsection 26WR(1) direction to an enforcement body, the consultation process under subsection 26WR(3) would ensure that the Commissioner is able to consider before issuing a subsection 26WR(1) direction whether the exception in new section 26WS is likely to apply.

Section 26WT Exception—inconsistency with prescribed secrecy provisions

198. This section makes clear how the requirement to comply with a subsection 26WR(1) direction interacts with secrecy provisions in other legislation. Different rules apply to particular secrecy provisions that have been prescribed in regulations under the Privacy Act for the purposes of this section.

199. This section is based on the exception in section 26WP above. It is expected that similar matters discussed in relation to section 26WP will be taken into account before prescribing secrecy provisions in regulations for the purposes of section 26WT.

Item 4 After paragraph 96(1)(b)

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

- under subsection 26WQ(7) above to refuse to give a subsection 26WQ(1) declaration on application by an entity that the entity is exempt from an obligation to notify an eligible data breach (which could include a decision refusing to grant declarations of a kind covered by paragraphs 26WQ(1)(c) or 26WQ(1)(d))

- under paragraph 26WQ(1)(d) above to give a declaration (which in practice would allow an entity to seek review where an entity nominates a particular period of time in an application for the Commissioner to make a declaration under paragraph 26WQ(1)(d), but the Commissioner makes a declaration for a shorter period of time), and

- under section 26WR above to give a subsection 26WR(1) direction to an entity to notify an eligible data breach

will be subject to review by the Administrative Appeals Tribunal.

Item 5 After subsection 96(2)

201. Item 5 of Schedule 1 inserts new subsections 96(2A), 96(2B), 96(2C) and 96(2D) into section 96 of the Privacy Act, after existing subsection 96(2).

202. The effect of subsections 96(2A), 96(2B) and 96(2C) is that paragraphs 96(1)(ba), 96(1)(bb) and 96(1)(bc) which are inserted by Item 4 above respectively provide that the only entity that can apply for review of the kind of a kind mentioned in those subsections is, for a decision falling under:

- paragraph 96(1)(ba), the entity who applied for the declaration that the Commissioner refused to grant under new subsection 26WQ(7), or another entity whose compliance with subsection 26WL(2) above is affected by the declaration (which is expected to operate where the eligible data breach to which the declaration relates is also an eligible data breach of another entity)

- paragraph 96(1)(bb), the entity to whom the declaration under paragraph 26WQ(1)(d) was given, or another entity whose compliance with subsection 26WL(2) is affected by the declaration (which is expected to operate where the eligible data breach to which the declaration relates is also an eligible data breach of another entity)

- paragraph 96(1)(bc), the entity to whom the subsection 26WR(1) direction was given.

203. Subsections 96(2A) and 96(2B) are primarily intended to operate so that, where an eligible data breach is an eligible data breach of one or more entities, each entity concerned is able to apply for AAT review of a decision by the Commissioner affecting their compliance with Part IIIC. Subsections 96(2A), 96(2B) and 96(2C) also prevent other individuals or parties from applying for AAT review of decisions falling under the new provisions inserted by Item 4 above: the intention is that, in terms of individuals whose information was subject to unauthorised access, unauthorised disclosure or loss in an eligible data breach, a complaint to the Commissioner under the Privacy Act about the eligible data breach, where grounds exist to make such a complaint, would be more appropriate than seeking AAT review of one of the above decisions.

204. Subsection 96(2D) provides that, for the purposes of subsections 96(2A), 96(2B) and 96(2C), 'entity' has the same meaning as in Part IIIC, which is defined in section 26WB above.

Item 6 Application of amendments—serious data breaches

205. Item 6 of Schedule 1 provides that Part IIIC to be inserted by this Bill applies to an access, disclosure, or loss that occurs after the commencement of Item 6. That is, none of the provisions in the Bill will operate retrospectively. Eligible data breaches that occur after the commencement date will be subject to the requirements of Part IIIC.