2013-2014

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

PRIVACY AMENDMENT (PRIVACY ALERTS) BILL 2014

EXPLANATORY MEMORANDUM

(Circulated by authority of Senator Singh)

PRIVACY AMENDMENT (PRIVACY ALERTS) BILL 2014

GENERAL OUTLINE

This Bill amends the *Privacy Act 1988* (**the Privacy Act**) to introduce mandatory data breach notification provisions for agencies and organisations that are regulated by the Privacy Act (**entities**).

Mandatory data breach notification commonly refers to a legal requirement to provide notice to affected persons and the relevant regulator when certain types of personal information are accessed, obtained, used, disclosed, copied, or modified by unauthorised persons. Such unauthorised access may occur following a malicious breach of the secure storage and handling of that information (e.g. a hacker attack), an accidental loss (most commonly of IT equipment or hard copy documents), a negligent or improper disclosure of information, or otherwise.

In its Report 108, *For Your Information: Australian Privacy Law and Practice*, the Australian Law Reform Commission (the **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.

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.

This Bill implements the ALRC's recommendation by requiring agencies and organisations regulated by the Privacy Act to provide notice to the Australian Information Commissioner (**the Commissioner**) and affected individuals of a serious data breach. The Bill contains general rules for the majority of entities regulated by the Privacy Act as well as analogous rules for credit reporting bodies and credit providers that are subject to specific regulation under Part IIIA, which deals with consumer credit reporting. The provisions in the Bill also apply to recipients of tax file number information. Each type of entity is subject to common requirements under the Privacy Act to protect the types of personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

A data breach arises where there has been unauthorised access to, or disclosure of, personal information, or where personal information is lost in circumstances that could give rise to unauthorised loss or disclosure. A data breach is a serious data breach where there is a *real risk of serious harm to the individual* to whom the information relates as a result of the breach. This is 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. In addition, the Bill provides for regulations to specify particular situations that may also be serious data breaches even if they do not necessarily reach the threshold of a real risk of serious harm. For example, this could include the release of particularly sensitive information such as health records which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection.

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

In the event of a serious data breach, the regulated entity is required to provide notification to the Commissioner and affected individuals as soon as practicable after the entity believes on reasonable grounds that there has been a serious data breach. The notice must include: the identity and contact details of the entity, a description of the serious data breach, the kinds of information concerned, recommendations about the steps that individuals should take in response to the serious data breach, and any other information specified in the regulations.

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 protect the security of their personal information. 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.

There may be circumstances in which it is impossible or impracticable to provide a notification to each affected individual. The Bill provides for regulations to be made describing those circumstances. If such regulations are made and the circumstances described in them are met, 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 and to publish the information in a newspaper circulating generally in each State and Territory.

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

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

In circumstances where the Commissioner believes that a serious data breach has occurred and no notification has been given by the entity that suffered the breach, the Commissioner may issue a written direction to the entity requiring it to provide notification of the data breach. The information to be provided to the Commissioner and affected individuals will be the same as if the entity had initiated the notification itself. Similarly, the requirements as to communicating with individuals will be the same. A law enforcement body that reasonably believes that compliance with the Commissioner's direction would be likely to prejudice law enforcement activities will be exempt from complying with the direction.

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 (including those that commenced in March 2014) to investigate, make determinations and provide remedies in relation to non-compliance with the Privacy Act. This includes the capacity to initiate own motion investigations, make determinations, seek enforceable undertakings, and pursue civil penalties for serious or repeated interferences with privacy.

This approach will permit the use of less severe sanctions before elevating to a civil penalty. These less severe penalties would follow a Commissioner's investigation and 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 a Court on application by the Commissioner.

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

NOTES ON CLAUSES

Preliminary

Clause 1—Short title

This clause provides that when the Bill is enacted, it may be cited as the *Privacy Amendment (Privacy Alerts) Act 2014*.

Clause 2—Commencement

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 the Royal Assent.

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 day to be fixed by proclamation, but that this must be within six months of the Royal Assent or the provisions will commence one day after this period.

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

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)

Item 1 of Schedule 1 inserts a definition of 'serious data breach' into existing subsection 6(1) of the Privacy Act. This item provides that the term 'serious data breach' has the meaning given by section 26X, 26Y, 26Z or 26ZA, which are inserted into the Privacy Act by this Bill (see item 4, below).

This definition is intended to capture data breaches that are significant enough to warrant notification. This will ensure the Government does not create or impose an unreasonable compliance burden on entities regulated by the scheme, and avoid the risk of 'notification fatigue' among individuals receiving a large number of notifications in relation to non-serious breaches.

Item 2

Item 2 of Schedule 1 inserts a definition of 'significantly affected' into existing subsection 6(1) of the Privacy Act. This item provides that the term 'significantly affected', in relation to an individual and in relation to a serious data breach, has the meaning given by section 26X, 26Y, 26Z or 26ZA, which are inserted into the Privacy Act by this Bill (see item 4, below).

This definition is intended to capture the individuals who are required to be notified in the event of a serious data breach. First, that will be individuals who are at real risk of serious harm in the event of a serious data breach. Secondly, it will also cover those individuals who are affected by serious data breaches involving particular categories of personal information, credit reporting information, credit eligibility information, or tax file number information that has been prescribed under the regulations (e.g. using the regulation-making power contained in subparagraph 26X(1)(d)(ii)).

Item 3 After subsection 13(4)

Item 3 of Schedule 1 inserts a new subsection 13(4A) into the Privacy Act after new subsection 13(4), as included by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (the **2012 Act**) (which commenced on 12 March 2014). New subsection 13(4A) is titled 'Data breach notification', and provides that if an entity (within the meaning of Part IIIC) contravenes either new section 26ZB or 26ZC of the Privacy Act (which are inserted by this Bill), the contravention is taken to be an act that is an 'interference with the privacy of an individual'. Subsection 6(1) of the Privacy Act, as amended by the 2012 Act, provides that the term 'interference with the privacy of an individual' has the meaning given by section 13 to 13F of the Privacy Act.

The effect of new subsection 13(4A) of the Privacy Act will be to enable the Australian Information Commissioner (the Commissioner) to use the powers and access the remedies available to the Commissioner under the Privacy Act to investigate and address contraventions of section 26ZB or 26ZC. These will include new powers that commenced on 12 March 2014. These include the capacity for the Commissioner to initiate own motion investigations, make determinations, seek enforceable undertakings, and pursue civil penalties for serious or repeated interferences with privacy.

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.

Item 4 After Part IIIB

Item 4 of Schedule 1 inserts a new Part IIIC, titled 'Data breach notification', 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.

The Part is divided into two Divisions. Broadly, the first Division sets out when a 'serious data breach' will have occurred, and the second Division contains obligations for entities to notify of that serious data breach, subject to limited exceptions.

Division 1—Serious data breach

Section 26X Serious data breach—APP entities

This section sets out the circumstances in which access to, or disclosure of, personal information will be a serious data breach where the personal information is held by an APP entity. 'APP entity' is defined in subsection 6(1) of the Privacy Act and includes Commonwealth government agencies and private sector organisations regulated by the Privacy Act. The provision refers to Australian Privacy Principle 11, which requires APP entities to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Unauthorised access or disclosure of personal information

New subsection 26X(1), which is titled 'Unauthorised access or disclosure of personal information', establishes the circumstances that will constitute a 'serious data breach' when personal information is subject to unauthorised access or unauthorised disclosure.

New subsection 26X(1) provides that unauthorised access to, or unauthorised disclosure of, personal information will be a serious data breach if an APP entity holds personal information relating to one or more individuals, is required under section 15 of the Privacy Act to comply with Australian Privacy Principle 11.1, and either:

- the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the personal information relates (subparagraph 26X(1)(d)(i)), or
- any of the personal information is of a kind specified in the regulations (subparagraph 26X(1)(d)(ii)).

In this context, 'serious harm' includes harm to reputation and economic or financial harm (section 26ZE). The risk of harm must be real (that is, not remote) for it to give rise to a serious data breach (section 26ZF). In order not to impose an unreasonable compliance burden on APP 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.

The ability to make regulations to specify particular situations that may also be serious data breaches is intended to provide the flexibility to deal with data breaches that may not reach the threshold of a real risk of serious harm but should nevertheless be subject to notification. These could include the release of particularly sensitive information such as health records which may not cause serious harm in every circumstance but should be subject to the highest level of privacy protection.

Paragraph 26X(1)(f) provides that, if subparagraph 26X(1)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is at real risk of serious harm from the access or disclosure of their personal information. Paragraph 26X(1)(g) provides that, if subparagraph 26X(1)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the personal information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26X(1) and before new subsection 26X(2). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

The effect of this section is to establish the circumstances that will constitute a 'serious data breach' when personal information is subject to unauthorised access or unauthorised disclosure.

Loss of personal information

New subsection 26X(2), which is titled 'Loss of personal information', establishes the circumstances that will constitute a 'serious data breach' when personal information is lost in a situation that may result in that personal information being subject to unauthorised access or unauthorised disclosure.

New subsection 26X(2) provides that the loss of personal information in circumstances where unauthorised access to, or unauthorised disclosure of, the personal information may occur will be a

serious data breach if an APP entity holds personal information relating to one or more individuals, is required under section 15 of the Privacy Act to comply with Australian Privacy Principle 11.1, and either:

- assuming that unauthorised access to, or unauthorised disclosure of, the personal information were to occur, the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the personal information relates (subparagraph 26X(2)(d)(i)), or
- any of the personal information is of a kind specified in the regulations (subparagraph 26X(2)(d)(ii)).

Paragraph 26X(2)(f) provides that, if subparagraph 26X(2)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual would be at real risk of serious harm if the unauthorised access or unauthorised disclosure of their personal information were to occur. Paragraph 26X(2)(g) provides that, if subparagraph 26X(2)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the personal information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26X(2) and before new subsection 26X(3). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

Overseas recipients

New subsection 26X(3), which is titled 'Overseas recipients', establishes the circumstances under which an APP entity will retain accountability for a 'serious data breach' involving personal information even though that APP entity might not be otherwise responsible for the breach due to the fact that the information has been disclosed to an overseas recipient.

New subsection 26X(3) provides that where:

- an APP entity has disclosed personal information to an overseas recipient
- APP 8.1 applied to that disclosure, and
- the overseas recipient holds the personal information,

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

Section 26Y Serious data breach—credit reporting bodies

This section sets out the circumstances in which unauthorised access to, or unauthorised disclosure of, credit reporting information will be a serious data breach where the credit reporting information is held by a credit reporting body. '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 and disclosed to credit reporting bodies. 'Credit reporting body' is defined in subsection 6(1) of the Privacy Act as an organisation that carries on a credit reporting business. The provision refers to

section 20Q of the Privacy Act. Section 20Q is based on APP 11 and requires credit reporting bodies to, among other things, protect credit reporting information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Unauthorised access or disclosure of credit reporting information

New subsection 26Y(1), which is titled 'Unauthorised access or disclosure of credit reporting information', establishes the circumstances that will constitute a 'serious data breach' when credit reporting information is subject to unauthorised access or unauthorised disclosure.

New subsection 26Y(1) provides that unauthorised access to, or unauthorised disclosure of, credit reporting information will be a serious data breach if a credit reporting body holds credit reporting information, is required to comply with section 20Q of the Privacy Act, and either:

- the unauthorised access or unauthorised disclosure will result in a real risk of serious harm to any of the individuals to whom the credit reporting information relates (subparagraph 26Y(1)(d)(i)), or
- any of the credit reporting information is of a kind specified in the regulations (subparagraph 26Y(1)(d)(ii)).

Paragraph 26Y(1)(f) provides that, if subparagraph 26Y(1)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is at real risk of serious harm from the access or disclosure of their credit reporting information. Paragraph 26Y(1)(g) provides that, if subparagraph 26Y(1)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the credit reporting information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26Y(1) and before new subsection 26Y(2). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

Loss of credit reporting information

New subsection 26Y(2), which is titled 'Loss of credit reporting information', establishes the circumstances that will constitute a 'serious data breach' when credit reporting information is lost in a situation that may result in that personal information being subject to unauthorised access or unauthorised disclosure.

New subsection 26Y(2) provides that the loss of credit reporting information in circumstances where unauthorised access to, or unauthorised disclosure of, the credit reporting information may occur will be a serious data breach if the credit reporting body holds credit reporting information relating to one or more individuals, is required to comply with section 20Q of the Privacy Act, and either:

- assuming that unauthorised access to, or unauthorised disclosure of, credit reporting information were to occur, the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the credit reporting information relates (subparagraph 26Y(2)(d)(i)), or
- any of the credit reporting information is of a kind specified in the regulations(subparagraph 26Y(2)(d)(ii)).

Paragraph 26Y(2)(f) provides that, if subparagraph 26Y(2)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual would be at real risk of serious harm if the unauthorised access to, or unauthorised disclosure of, the credit reporting information were to occur. Paragraph 26Y(2)(g) provides that, if subparagraph 26Y(2)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the credit reporting information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26Y(2) and before new subsection 26Y(3). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

Section 26Z Serious data breach—credit providers

This section sets out the circumstances in which access to or disclosure of credit eligibility information will be a serious data breach where the credit eligibility information is held by a credit provider. 'Credit eligibility information' is defined in subsection 6(1) of the Privacy Act as including credit reporting information disclosed to a credit provider by a credit reporting body and information derived from the credit reporting information. 'Credit provider' is defined in section 6G of the Privacy Act as including a bank or other organisation that provides credit as a substantial part of its business or undertaking. The provision refers to section 21S of the Privacy Act. Section 21S is based on APP 11 and requires credit providers, among other things, to protect credit eligibility information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Unauthorised access or disclosure of credit eligibility information

New subsection 26Z(1), which is titled 'Unauthorised access or disclosure of credit eligibility information', establishes the circumstances that will constitute a 'serious data breach' when credit eligibility information is subject to unauthorised access or unauthorised disclosure.

New subsection 26Z(1) provides that unauthorised access to, or unauthorised disclosure of, credit eligibility information will be a serious data breach if a credit provider holds credit eligibility information, is required to comply with subsection 21S(1) of the Privacy Act, and either:

- the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the credit eligibility information relates (subparagraph 26Z(1)(d)(i)), or
- any of the credit eligibility information is of a kind specified in the regulations (subparagraph 26Z(1)(d)(ii)).

Paragraph 26Z(1)(f) provides that, if subparagraph 26Z(1)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is at real risk of serious harm from the access or disclosure of their credit eligibility information. Paragraph 26Z(1)(g) provides that, if subparagraph 26Z(1)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the credit eligibility information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26Z(1) and before new subsection 26Z(2). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

Loss of credit eligibility information

New subsection 26Z(2), which is titled 'Loss of credit eligibility information', establishes the circumstances that will constitute a 'serious data breach' when personal information is lost in a situation that may result in that credit eligibility information being subject to unauthorised access or unauthorised disclosure.

New subsection 26Z(2) provides that the loss of credit eligibility information in circumstances where unauthorised access to, or unauthorised disclosure of, the credit eligibility information may occur will be a serious data breach if the credit provider holds credit eligibility information relating to one or more individuals, is required to comply with section 21S(1) of the Privacy Act, and either:

- assuming that unauthorised access to, or unauthorised disclosure of, credit eligibility information were to occur, the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the credit eligibility information relates (subparagraph 26Z(2)(d)(i)), or
- any of the credit eligibility information is of a kind specified in the regulations (subparagraph 26Z(2)(d)(ii)).

Paragraph 26Z(2)(f) provides that, if subparagraph 26Z(2)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual would be at real risk of serious harm if the unauthorised access to, or unauthorised disclosure of, the credit eligibility information were to occur. Paragraph 26Z(2)(g) provides that, if subparagraph 26Z(2)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the credit eligibility information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26Z(2) and before new subsection 26Z(3). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

Bodies or persons with no Australian link

New subsection 26Z(3), which is titled 'Bodies or persons with no Australian link', establishes the circumstances under which a credit provider will retain accountability for a 'serious data breach' involving credit eligibility information that was disclosed to a body or person with no Australian link.

New subsection 26Z(3) provides that where:

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

then new section 26Z of the Privacy Act applies to that transfer of credit eligibility information as if the credit eligibility information were held by the credit provider, and the credit provider were required to comply with subsection 21S(1) of the Privacy Act in relation to the credit eligibility

information. This means that the requirements of new subsections 26Z(1) and 26Z(2) apply, and the credit provider retains accountability for that credit eligibility information, even where a credit provider discloses credit eligibility information to a recipient that does not have an Australian link. The term 'Australian link' is used to define the entities that are subject to the operation of the Privacy Act, and is used, for example, in new 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.

This item also inserts a note following new subsection 26Z(3) and before new section 26ZA. The note provides a cross-reference to section 21NA of the Privacy Act. That section provides that credit providers may, where they satisfy the requirements of clause 21NA, disclose credit eligibility information to an entity that does not have an Australian link. Types of overseas entities to which a credit provider may choose to disclose credit eligibility information may include a credit provider's agents or related body corporates, as well as a credit provider's credit managers or debt collectors.

Section 26ZA Serious data breach—file number recipients

This section sets out the circumstances in which unauthorised access to, or unauthorised disclosure of, tax file number information will be a serious data breach where the tax file number information is held by a file number recipient. 'Tax file number' and 'tax file number information' are defined in section 6(1) of the Privacy Act. The provision refers to sections 17 and 18 of the Privacy Act. Section 17 provides that the Commissioner must issue guidelines concerning the collection, storage, use and security of tax file number information. Section 18 provides that a file number recipient shall not do an act, or engage in a practice, that breaches a guideline issued under section 17.

Unauthorised access or disclosure of tax file number information

New subsection 26ZA(1), which is titled 'Unauthorised access or disclosure of tax file number information', establishes the circumstances that will constitute a 'serious data breach' when tax file number information is subject to unauthorised access or unauthorised disclosure.

New subsection 26ZA(1) provides that unauthorised access to, or unauthorised disclosure of, tax file number information will be a serious data breach if a file number recipient holds tax file number information, is required to comply with sections 17 and 18 of the Privacy Act, and either:

- the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the tax file number information relates (subparagraph 26ZA(1)(d)(i)), or
- any of the credit eligibility information is of a kind specified in the regulations (subparagraph 26ZA(1)(d)(ii)).

New paragraph 26ZA(1)(f) provides that, if subparagraph 26ZA(1)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is at real risk of serious harm because of the unauthorised access to, or unauthorised disclosure of, their tax file number information. Paragraph 26ZA(1)(g) provides that, if subparagraph 26ZA(1)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the tax file number information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26ZA(1) and before new subsection 26ZA(2). Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

Loss of tax file number information

New subsection 26ZA(2), which is titled 'Loss of tax file number information', establishes the circumstances that will constitute a 'serious data breach' when tax file number information is lost in a situation that may result in that personal information being subject to unauthorised access or unauthorised disclosure.

New subsection 26ZA(2) provides that the loss of tax file number information in circumstances where unauthorised access to, or unauthorised disclosure of, the tax file number information may occur will be a serious data breach if the file number recipient holds tax file number information relating to one or more individuals; is required to comply with sections 17 and 18 of the Privacy Act, and either:

- assuming that unauthorised access to, or unauthorised disclosure of, tax file number information were to occur, the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the credit eligibility information relates (subparagraph 26ZA(2)(d)(i)), or
- any of the tax file number information is of a kind specified in the regulations (subparagraph 26ZA(2)(d)(ii)).

Paragraph 26ZA(2)(f) provides that, if subparagraph 26ZA(2)(d)(i) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual would be at real risk of serious harm if the unauthorised access to, or unauthorised disclosure of, the tax file number information were to occur. Paragraph 26ZA(2)(g) provides that, if subparagraph 26ZA(2)(d)(ii) applies, an individual is 'significantly affected' by the serious data breach if, and only if, the individual is both an individual to whom the tax file number information relates; and an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

This item also inserts two notes following new subsection 26ZA(2) and before the heading for new Division 2—Notifying serious data breaches. Note 1 provides a cross-reference to the definition of the term 'harm' in new section 26ZE. Note 2 provides a cross-reference to the definition of the term 'real risk' in new section 26ZF.

Division 2—Notifying serious data breaches

Section 26ZB Entity must notify serious data breach

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

New subsection 26ZB(1) provides that if an entity believes on reasonable grounds that there has been a serious data breach of the entity in relation to either personal information, credit reporting information, credit eligibility information or tax file number information, the entity must, as soon as practicable after forming that belief:

- prepare a statement that complies with new subsection 26ZB(2) (paragraph 26ZB(1)(e)) (a **paragraph 26ZB(1)(e) statement**)

- give a copy of the paragraph 26ZB(1)(e) statement to the Commissioner (paragraph 26ZB(1)(f))
- if the general publication conditions are not satisfied, take such steps as are reasonable in the circumstances to notify the contents of the paragraph 26ZB(1)(e) statement to each of the individuals significantly affected by the serious data breach that the entity believes has happened (paragraph 26ZB(1)(g)), and
- if the general publication conditions are satisfied:
    - publish a copy of the paragraph 26ZB(1)(e) statement on the entity's website (if any) (subparagraph 26ZB(1)(h)(i)), and
    - cause a copy of the statement to be published in each State by being published in at least one newspaper circulating generally in that State (subparagraph 26ZB(1)(h)(ii)).

This item also inserts a note following new subsection 26ZB(1) and before new subsection 26ZB(2). The note provides a cross-reference to subsection 26ZB(12), which contains the general publication conditions.

The concept in paragraph 26ZB(1)(g) of 'taking such steps as are reasonable in the circumstances' is used elsewhere in the Privacy Act. As noted in the Explanatory Memorandum to the Bill for the 2012 Act, 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.

This flexibility is necessary given the different types of entities that are to be regulated under the new scheme. For example, for entities with particular functions or engaged in certain activities, it may not be 'reasonable in the circumstances' to notify about a data breach. For example, it may not be reasonable in the circumstances for a Commonwealth agency or private sector organisation to notify particular individuals about a data breach, where that organisation has been advised by a law enforcement agency or intelligence agency that notification might prejudice or adversely affect a law enforcement investigation or intelligence related activity. However, the entity would still be required to comply with paragraph 26ZB(1)(f) and provide a copy to the Commissioner.

New subsection 26ZB(2) sets out the contents of the paragraph 26ZB(1)(e) statement that an entity must prepare to give notice of a serious data breach. These are based on the matters in the current OAIC *Data Breach Notification: A guide to handling personal information security breaches*. The statement must include:

- the identity and contact details of the entity (paragraph 26ZB(2)(a))
- a description of the serious data breach that the entity believes has happened (paragraph 26ZB(2)(b))
- the kinds of information concerned (paragraph 26ZB(2)(c)) recommendations about the steps that individuals should take in response to the data breach that the entity believes has happened (paragraph 26ZB(2)(d)), and
- any other information (if any) as specified in the regulations (paragraph 26ZB(2)(e)).

This means that, if the conditions in any regulations are met, instead of taking steps to notify each individual about the contents of the paragraph 26ZB(1(e) statement, the entity may make a general publication in relation to the serious data breach. New subsection 26ZB(12) provides that the regulations may declare one or more specified conditions to be general publication conditions. It is envisaged that the regulations will deal with situations where it is impossible for the entity to contact

each affected individual or where an attempt to contact each individual would be ineffective. Paragraph 26ZB(1)(h) provides that where an entity makes a general publication it must publish a copy of the notification on its website (if it has one) and cause a copy of the notification to be published in each State in at least one newspaper circulating generally in that State.

Method of providing the statement to an individual

Without limiting paragraph 26ZB(1)(g), new subsection 26ZB(3), 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 26ZB(1)(g) may use that method. This is intended to reduce the cost of compliance for entities but also to ensure that individuals receive notifications through communication channels that they expect relevant entities to use. Where there is no normal mode of communication with the particular individual the entity must take reasonable steps to communicate with him or her. Reasonable steps could include contact by email, telephone or post.

Exception—enforcement related activities

New subsection 26ZB(4), which is titled 'Exception—enforcement related activities', provides that new paragraphs 26ZB(1)(g) and 26ZB(1)(h) of the Privacy Act do not apply if the relevant entity is a law enforcement body that believes on reasonable grounds that compliance with those paragraphs would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, the enforcement body.

'Enforcement body' and 'enforcement related activities' are defined in subsection 6(1) of the Privacy Act. The effect of this provision is that a law enforcement body is not required to notify affected individuals of the contents of the paragraph 26ZB(1)(e) statement, either individually or in compliance with the general publication conditions specified in subsection 26ZB(12). However, the entity must still comply with paragraphs 26ZB(1)(e) (i.e., the entity must prepare a statement that complies with new subsection 26ZB(2)) and 26ZB(1)(f) (i.e. the entity must give a copy of that statement to the Commissioner).

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 toserious data breaches that are not related to enforcement activities such as the inadvertent disclosure of personal information unrelated to investigations or intelligence gathering. It also ensures that notification to the Commissioner is still required, so that the Commissioner can advise and assist enforcement bodies in responding to data breaches, and can continue to collect important information about data breaches to assist in combating or addressing them into the future.

Exception—Commissioner's notice

New subsection 26ZB(5), which is titled 'Exception—Commissioner's notice', provides that the Commissioner may, by written notice given to an entity, exempt that entity from the requirement to notify contained in new subsection 26ZB(1), in such circumstances that are contained in that written notice (a **subsection 26ZB(5) notice**).

New subsection 26ZB(6) provides that a subsection 26ZB(5) notice can only be given when the Commissioner is satisfied that it is in the public interest to do so. It is expected that the Commissioner

will develop guidance in consultation with agencies and organisations on what factors will need to be taken into account in determining whether issuing a notice will be in the public interest.

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

New subsection 26ZB(7) provides that the Commissioner may issue a subsection 26ZB(5) notice either on the Commissioner's own initiative or on application made by the entity. A decision by the Commissioner to refuse to issue a subsection 26ZB(5) notice will be reviewable by the Administrative Appeals Tribunal (see item 5 below).

New subsection 26ZB(8) provides that, where the Commissioner refuses an application made by an entity under paragraph 26ZB(7)(b) for a subsection 26ZB(5) notice, the Commissioner must give written notice of the refusal.

New subsection 26ZB(9) provides that, if an entity forms a belief that a serious data breach has occurred (paragraph 26ZB(9)(a)), and, as soon as practicable after forming that belief, the entity applies to the Commissioner for a subsection 26ZB(5) notice (paragraph 26ZB(9)(b)); the requirement to notify contained in new subsection 26ZB(1) will not apply during the period beginning when the entity formed the belief that a serious data breach has occurred, and ending when the Commissioner makes a decision about the application (paragraph 26ZB(9)(c)). This provision is intended to make it clear that the entity will not be in breach of notification obligations while its application for a subsection 26ZB(5) notice is being considered by the Commissioner.

New paragraph 26ZB(9)(d) provides that if the Commissioner decides to refuse to give a subsection 26ZB(5) notice, subsection 26ZB(1) applies from the date of the Commissioner's decision. That is, where the Commissioner refuses an application for a subsection 26ZB(5) notice, the entity must comply with its obligations under paragraphs 26ZB(1)(e) – (h) as soon as practicable following that decision.

Exception—inconsistency with secrecy provisions

New subsection 26ZB(10), which is titled 'Exception—inconsistency with secrecy provisions', provides that, if compliance by an entity with paragraph 26ZB(1)(f), (g) or (h) of the Privacy Act would, to any extent, be inconsistent with a provision of a law of the Commonwealth (other than a provision of the Privacy Act) that prohibits or regulates the use or disclosure of information, the requirement to notify contained in subsection 26ZB(1) does not apply to the entity to the extent of the inconsistency.

The effect of this provision is to make it clear that the secrecy provisions contained in other Commonwealth legislation prevails over the requirement to notify in subsection 26ZB(1) of the Privacy Act. For example, subsection 26ZB(10) will ensure that there is no conflict between the Privacy Act and the provisions of other acts which prohibit disclosure of official information or secrets by Commonwealth officers (such as sections 70 and 79 of the *Crimes Act 1914* (Cth)).

Exception—data breach notified under Personally Controlled Electronic Health Records Act 2012

New subsection 26ZB(11), which is titled 'Exception— data breach notified under *Personally Controlled Electronic Health Records Act 2012*', provides that subsection 26ZB(1) does not apply to a serious data breach if the breach has been notified under section 75 of the Personally *Controlled Electronic Health Records Act 2012* (**PCEHR Act**). This provision has the effect of preventing the imposition of a double notification requirement on entities that have complied with section 75 of the PCEHR Act in relation to the same data breach.

General publication conditions

New subsection 26ZB(12), which is titled 'General publication conditions', provides that the regulations may declare that one or more specified conditions are general publication conditions for the purposes of new section 26ZB of the Privacy Act. It is envisaged that the regulations will deal with situations where it is impossible for the entity to contact each affected individual or where an attempt to contact each individual would be ineffective.

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

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

New subsection 26ZC(1) provides that if the Commissioner believes on reasonable grounds that there has been a serious data breach of the entity in relation to either personal information, credit reporting information, credit eligibility information or tax file number information, the Commissioner may, by written notice given to the entity, direct the entity to:

- prepare a statement that complies with new subsection 26ZC(2) (paragraph 26ZC(1)(e)) (a **paragraph 26ZC(1)(e) statement**)
- give a copy of the paragraph 26ZC(1)(e) statement to the Commissioner (paragraph 26ZC(1)(f))
- if the general publication conditions are not satisfied, take such steps as are reasonable in the circumstances to notify the contents of the paragraph 26ZC(1)(e) statement to each of the individuals significantly affected by the serious data breach that the Commissioner believes has happened (paragraph 26ZC(1)(g)), and
- if the general publication conditions are satisfied:
    - publish a copy of the paragraph 26ZC(1)(e) statement on the entity's website (if any), (subparagraph 26ZC(1)(h)(i)), and
    - cause a copy of the paragraph 26ZC(1)(e) statement to be published in each State by being published in at least one newspaper circulating generally in that State (subparagraph 26ZC(1)(h)(ii)).

This item also inserts a note following new subsection 26ZC(1) and before new subsection 26ZC(2). The note provides a cross-reference subsection 26ZC(8), which provides general publication conditions.

New subsection 26ZC(2) sets out the contents of the paragraph 26ZC(1)(e) statement that an entity must prepare to give notice of a serious data breach. These are based on the matters in the current

OAIC *Data Breach Notification: A guide to handling personal information security breaches*. The paragraph 26ZC(1)(e) statement must include:

- the identity and contact details of the entity (paragraph 26ZC(2)(a))
- a description of the serious data breach that the Commissioner believes has happened (paragraph 26ZC(2)(b))
- the kinds of information concerned (paragraph 26ZC(2)(c))
- recommendations about the steps that individuals should take in response to the data breach that the Commissioner believes has happened (paragraph 26ZC(2)(d)), and
- any other information (if any) as specified in the regulations (paragraph 26ZC(2)(e)).

This means that, if the conditions in any regulations are met, instead of taking steps to notify each individual, the entity may make a general publication in relation to the serious data breach. New subsection 26ZC(8) provides that the regulations may declare one or more specified conditions to be general publication conditions. It is envisaged that the regulations will deal with situations where it is impossible for the entity to contact each affected individual or where an attempt to contact each individual would be ineffective. Paragraph 26ZC(1)(h) provides that where an entity makes a general publication it must publish a copy of the notification on its website (if it has one) and cause a copy of the notification to be published in each State in at least one newspaper circulating generally in that State.

Method of providing the statement to an individual

Without limiting paragraph 26ZC(1)(g), new subsection 26ZC(3), 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 26ZC(1)(g) may use that method. This is intended to reduce the cost of compliance for entities but also to ensure that individuals receive notifications through communication channels that they expect relevant entities to use. Where there is no normal mode of communication with the particular individual the entity must take reasonable steps to communication with him or her. Reasonable steps could include contacting by email, telephone or post.

Compliance with direction

New subsection 26ZC(4), which is titled 'Compliance with direction', provides that an entity must comply with a direction given by the Commissioner under subsection 26ZC(1) (a **subsection 26ZC(1) direction**) as soon as practicable after the direction is given.

Exception—enforcement related activities

New subsection 26ZC(5), which is titled 'Exception—enforcement related activities', provides that the Commissioner must not give a subsection 26ZC(1) direction to an entity that is a law enforcement body if the chief executive officer of that law enforcement body has given the Commissioner a certificate stating that the enforcement body believes on reasonable grounds that compliance with the direction would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body.

'Enforcement body' and 'enforcement related activities' are defined in subsection 6(1) of the Privacy Act. This exception is intended to ensure that the legitimate activities of enforcement bodies are not disrupted or affected by the notification requirement. However, it does not extend to serious data

breaches that are not related to enforcement activities such as the inadvertent disclosure of personal information unrelated to investigations or intelligence gathering. The requirement that the chief executive of the enforcement body provide the Commissioner with a certificate will ensure that the Commissioner can be assured that the enforcement body has formed the relevant belief on reasonable grounds.

This exception will apply in relation to notification to individuals. As noted above, the effect of subclause 26ZB(4) is that an enforcement body will still be required to notify all serious data breaches to the Commissioner. The exception in subclause 26ZC(5) does not exempt an enforcement body from that requirement.

Exception—inconsistency with secrecy provisions

New subsection 26ZC(6), which is titled 'Exception—inconsistency with secrecy provisions', provides that, if compliance by an entity with a subsection 26ZC(1) direction as is covered by paragraph 26ZC(1)(f), (g) or (h) would, to any extent, be inconsistent with a provision of a law of the Commonwealth (other than a provision of this Act) that prohibits or regulates the use or disclosure of information, paragraph 26ZC(1)(f), (g) or (h), as the case may be, does not apply to the entity to the extent of the inconsistency.

The effect of this provision is to make it clear that the secrecy provisions contained in other Commonwealth legislation prevails over the requirement to comply with a subsection 26ZC(1) direction. For example, subsection 26ZC(6) will ensure that there is no conflict between the Privacy Act and the provisions of other acts which prohibit disclosure of official information or secrets by Commonwealth officers (such as sections 70 and 79 of the *Crimes Act 1914* (Cth)).

Exception— data breach notified under Personally Controlled Electronic Health Records Act 2012

New subsection 26ZC(7), which is titled 'Exception— data breach notified under *Personally Controlled Electronic Health Records Act 2012*', provides that the Commissioner must not give a subsection 26ZC(1) direction in relation to a serious data breach if the breach has been notified under section 75 of the PCEHR Act. This provision has the effect of preventing the imposition of a double notification requirement on entities that have complied with section 75 of the PCEHR Act in relation to the same data breach.

General publication conditions

New subsection 26ZC(8), which is titled 'General publication conditions', provides that the regulations may declare that one or more specified conditions are general publication conditions for the purposes of new section 26ZC of the Privacy Act. It is envisaged that the regulations will deal with situations where it is impossible for the entity to contact each affected individual or where an attempt to contact each individual would be ineffective.

Division 3—General

Section 26ZD Entity

Section 26ZD provides that, for the purposes of the new Part IIIC—Data breach notification, 'entity' includes a person who is a file number recipient.

Section 26ZE Harm

Section 26ZE provides that, for the purposes of the new Part IIIC—Data breach notification, the word 'harm' includes harm to reputation, economic harm, and financial harm. This is a non-exhaustive list and is in addition to the ordinary meaning of the word 'harm'. The section is included to provide clarity.

Section 26ZF Real risk

Section 26ZF provides that, for the purposes of the new Part IIIC—Data breach notification, the term 'real risk' means a risk that is not a remote risk.

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

Item 5 After paragraph 96(1)(b)

Item 5 of Schedule 1 inserts new paragraphs 96(1)(ba) and 96(1)(bb) into subsection 96(1) of the Privacy Act, after existing paragraph 96(1)(b). The effect of this insertion is that new paragraphs 96(1)(ba) and 96(1)(bb) respectively provide that a decision by the Commissioner:

- under section 26ZB to refuse to give a subsection 26ZB(5) notice that an entity is exempt from an obligation to notify a serious data breach, and
- under section 26ZC to give a subsection 26ZC(1) direction to an entity to notify a serious data breach will be subject to review by the Administrative Appeals Tribunal.

Item 6 Application of amendments—serious data breaches

Item 6 of Schedule 1 provides that the new Part IIIC of the Privacy Act to be inserted by this Bill applies to the access, disclosure, or loss of personal information, as well as credit reporting information, credit eligibility information and tax file number information that occurs after the commencement of item 6. That is, none of the provisions in the Bill will operate retrospectively. Serious data breaches that occur after commencement will be subject to the requirements of the new Part IIIC.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

Privacy Amendment (Privacy Alerts) Bill 2014

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

The Bill amends the *Privacy Act 1988* by inserting provisions imposing a data breach notification requirement on entities regulated by Privacy Act (entity) in relation to serious data breaches.

'Serious data breach' is defined in the Bill. Broadly speaking, a data breach occurs where personal information held by an entity is subject to unauthorised access or disclosure. A hacking attack involving the publication online of individuals' names and credit card numbers would be an example of a 'serious data breach'. Another example would be the accidental publication of patient records by a medical practice.

The Bill provides that, where an entity has suffered a serious data breach, it must notify the individual(s) whose personal information is the subject of the breach (affected individuals) as well as the Australian Information Commissioner.

In addition, the Commissioner may direct an entity to notify affected individuals of a serious data breach. The Bill provides that an entity which fails to notify affected individuals engages in an interference with the privacy of an individual. The Commissioner may pursue a civil penalty on such an entity under the new reforms to the Privacy Act, which commenced on 12 March 2014.

The Bill's notification requirements are expected to result in more timely opportunities for individuals to promptly respond to a data breach by changing passwords, cancelling credit cards etc. 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

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

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.

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 a 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.

Law enforcement exemption

The notification requirement will be limited where: (a) the entity is an enforcement body; and (b) the enforcement body believes on reasonable grounds that compliance with that subsection 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. 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 law enforcement bodies are not exempt from the notification requirement as such. They will still have to comply with the notification requirement in circumstances where compliance would not prejudice an enforcement related activity.

The right to a fair trial

The Bill engages 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 penalties provided for by the Bill.

As noted above, the Bill provides that an entity which fails to notify affected individuals of a serious 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. Other interferences as defined in the amended Privacy Act include 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. A civil penalty can only be issued by the Federal Court or 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 penalties that may be imposed under the Privacy Act upon entities which have committed interferences with the privacy of an individual are compatible with Article 14 of the ICCPR. The penalties are further explained in the Statement of Compatibility with Human Rights for the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* at pages 44–49 of the Explanatory Memorandum for the Bill for that Act.

Conclusion

The Bill is compatible with human rights because it promotes the right to privacy in Article 17, and does not interfere with the rights protected by Article 14, of the ICCPR.