Australian Broadcasting Corporation

Response to

Attorney-General's Department Discussion Paper

Mandatory data breach notification

December 2015

ABC

ABC Response to Attorney-General's Department Discussion Paper

Mandatory data breach notification

December 2015

Introduction

The ABC welcomes the opportunity to respond to the Attorney-General's Department discussion paper on mandatory data breach notification, issued in December 2015. The ABC supports in principle the creation of a legal requirement on agencies and organisations to notify the Australian Information Commissioner and affected individuals when a serious data breach occurs which will result in a real risk of serious harm to those individuals.

In making this submission, the ABC has had regard to the following documents:

- Discussion paper—Mandatory data breach notification
- Exposure draft—*Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*
- Explanatory memorandum— *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*
- Draft Early Assessment Regulatory Impact Statement—*Privacy Amendment (Notification of Serious Data Breaches) Bill 2015.*

The ABC will confine its comments to a small number of specific concerns in relation to the Exposure draft—*Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* (the "draft Bill").

Awareness of a serious data breach

Under s.26WC(1) as proposed in the draft Bill, an entity is required to prepare a statement that complies with s.26WC(3) 'as soon as practicable' after the entity becomes aware or 'ought reasonably to be aware' that there has been a serious data breach. Proposed s.26WC(2) also refers to the time at which an entity 'ought reasonably to be aware' of a serious data breach as one of the triggers for carrying out a 'reasonable assessment of whether there are reasonable

grounds to believe that the relevant circumstances amount to a serious data breach'.

The ABC submits that the requirement to issue a statement under proposed s.26WC(3) of the draft Bill should only be triggered when an entity becomes aware of a serious data breach, not from when an entity 'ought reasonably to be aware' that a serious data breach has occurred. Having regard to the current threat landscape, the practical reality of sophisticated cyber-attacks is that an entity may not become aware of a serious data breach until after the hacked information has been unlawfully used or disclosed. This may be a significant time after the serious data breach occurred. According to a recent study from the cybersecurity firm FireEye, organisations take, on average, 229 days to detect a data breach and two-thirds of organisations are informed about the breach by a third party. In those circumstances, it will be difficult to determine the point at which the entity 'ought reasonably to be aware' of the serious data breach.

Time period for making an assessment

Under s.26WC(2) as proposed in the draft Bill, a 'reasonable assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to a serious data breach' must be carried out within 30 days after the entity becomes aware of a serious data breach or 'ought reasonably to have become so aware'.

The ABC reiterates its submission above regarding the inclusion of the phrase 'ought reasonably to have become so aware'.

Further, the ABC submits that the draft Bill should be amended to include a process to enable the Commissioner to grant an extension of time on application from an entity in circumstances where the assessment of whether there has been a serious data breach involves a complex investigation, for example because the potential data breach is highly technical in nature, or extends across more than one entity.

Overseas recipients

Under s.26WB(5) as proposed in the draft Bill, the notification obligations in relation to a 'serious data breach' extend to a data breach that occurs in relation to personal information that is held by an overseas recipient by virtue of Australian Privacy Principle (APP) 8.1 (cross-border disclosure).

Section 26WB(5) as proposed in the draft Bill appears to be consistent in principle with s.16C of the *Privacy Act 1988*. However, the provisions are drafted in slightly different terms, and there is a risk that the two provisions may create confusion or uncertainty. For instance, proposed s.26WB(5) introduces a new concept of an overseas recipient 'holding' personal information. The ABC submits that the draft Bill should be amended to either remove proposed s.26WB(5) or to ensure that its application is clear and consistent with s.16C of the *Privacy Act 1988*.

Further, as presently drafted, proposed s.26WB(5) imposes an absolute obligation on an entity to issue a statement in accordance with proposed s.26WC(3) in the event of a serious data breach of personal information held by an overseas recipient by virtue of APP 8.1. This obligation exists regardless of whether an entity is made aware of a serious data breach by the overseas recipient. It is feasible that an entity may take reasonable steps to ensure that an overseas

recipient is required to notify the entity of a serious data breach (for instance, by imposing contractual obligations to that effect), but may nevertheless be unaware of a serious data breach by the overseas recipient (for instance, if the overseas recipient fails to comply with the contractual obligation). In those circumstances, the entity will be unable to comply with proposed s.26WC(3) despite having taken reasonable steps to do so.

This is inconsistent with the approach taken to the management of cross-border disclosure of personal information in APP 8.1 which requires an APP entity to 'take such steps as are reasonable in the circumstances'. The ABC submits that further consideration should be given to addressing this inconsistency. In making this submission the ABC reiterates the contention outlined above that the requirement to issue a statement under proposed s.26WC(3) of the draft Bill should only be triggered when an entity becomes aware of a serious data breach, not from when an entity 'ought reasonably to be aware' that a serious data breach has occurred.

Direction from Commissioner

Under s.26WD as proposed in the draft Bill, the Commissioner may direct an entity to prepare a statement that complies with subsection (2) if he or she 'believes on reasonable grounds that there has been a serious data breach' of the entity.

The required statement must include:

- A description of the serious data breach that the Commissioner believes has happened;
- The kind or kinds of information concerned; and
- Recommendations about the steps that individuals should take in response to the serous data breach that the Commissioner believes has happened.

The ABC does not disagree in principle with an entity being required to issue a data breach notification on direction from the Commissioner. However, as drafted the circumstances in which that may occur, and the process to be followed, overlook some fundamental elements and would potentially result in a lack of procedural fairness. Amendments to the draft Bill are required to enable an entity to meet the requirements of s.26WD(2).

Firstly, the draft Bill does not explicitly require the Commissioner to provide an entity with details of the nature of the serious data breach, or the grounds on which the Commissioner believes there has been a serious data breach. Without this information it is not feasible for an entity to issue the required statement. The ABC submits that the draft Bill should be amended to include a requirement that the Commissioner provide such information about the serious data breach and the grounds on which the Commissioner believes there has been such a breach as may be reasonably required to enable an entity to prepare and issue the required statement.

Second, the draft Bill does not provide any mechanism for an entity to question or dispute a direction from the Commissioner. The ABC submits that the draft Bill should include an appropriate process to enable an entity to request that the Commissioner review his or her decision to issue a direction if the entity considers that either (a) the data breach was not a serious data breach; and/or (b) that there are not reasonable grounds to believe that there has been a serious data breach.

Harm

Section 26WF as proposed in the draft Bill defines 'harm' for the purposes of proposed Part IIIC (Notification of serious data breaches). 'Harm' is defined to include:

- physical harm
- psychological harm
- emotional harm
- harm to reputation
- economic harm
- financial harm.

The ABC submits that psychological harm and emotional harm will be difficult to assess. A person who is particularly emotionally or psychologically vulnerable may be more likely to suffer emotional or psychological harm as a result of a serious data breach. Applying the general principle that an entity should 'take their victims as they find them', it is unclear how an entity should determine whether there is a 'real risk of serious harm to an individual' if the individual's sensitivity to emotional or psychological harm is unknown.

The ABC further submits that harm to reputation involves speculation and subjectivity, and will be difficult to determine. It is not clear what is meant by 'economic harm'.

The ABC submits that proposed s.26WF be removed from the draft Bill. Alternatively, the definition of 'harm' should be limited to physical harm and financial harm.