SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS
ATTORNEY-GENERAL'S PORTFOLIO

Group: 3

Program: 1.6

Question No. SBE14/157

Senator Collins asked the following question at the hearing on 20 November 2014:

1. When did the Government decide to remove the requirement for ministerial approval of storage by Government agencies of Australians' personal information in overseas cloud facilities? Where is this decision recorded?

2. How will Australian privacy law apply where government data is stored by private providers overseas?

3. What remedies will be available to Australians if there is a data leak from an offshore data centre?

4. Will affected individuals be notified that their personal data is being held overseas?

The answer to the honourable senator's question is as follows:

1. The removal of the policy requiring dual ministerial approval occurred in August 2014 following a review of the *Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced of offshore ICT arrangements* (the Policy). The policy was replaced with a set of enhanced guidelines to provide Australian Government agencies with a consistent approach to assessing and managing the risks associated with outsourced ICT arrangements, including cloud services.

   As the Minister for protective security policy, this decision was approved by the Attorney-General in consultation with the Department of Communications and the Australian Government Information Management Office (AGIMO); with extensive industry engagement.

   The Protective Security Policy Framework (PSPF) sets the appropriate measures for Australian Government agencies to protect its people, information and assets. Agency Heads remain responsible for the management of the risk within their agency, including the risk associated with any decision to store or process Australian government information in an outsourced or offshore ICT arrangement.

   There is no change to the safeguarding requirements for information held in trust by Australian Government agencies. Agencies must manage their information holdings under the obligations of the Privacy Act 1988 and the Australian Privacy Principles relating to the handling and safeguarding of 'personal' information.

2. Commonwealth Government agencies and private sector organisations that are not otherwise exempt must comply with the Australian Privacy Principles (APPs) in the

Privacy Act 1988. The APPs provide general rules that deal with the management, collection, use, disclosure, and handling of personal information. Section 95B requires government agencies to take contractual measures to ensure that contracted service providers do not do acts or engage in practices that would breach the APPs.

APP 8 and s 16C of the Privacy Act create a framework for the cross-border disclosure of personal information and require entities (which include government agencies) to ensure that overseas recipients handle personal information in accordance with the APPs. These provisions also ensure that the Australian entity is accountable if the overseas recipient mishandles the personal information. Additionally, entities must ensure that they comply with all other relevant APPs, including APP 1 (which requires the entity's privacy policy to include whether it is likely any personal information will be disclosed to overseas recipients), APP 5 (which requires notice to be given to individuals, including of any cross-border disclosures), APP 6 (which sets out the general circumstances in which personal information can be used or disclosed), and APP 11 (which requires personal information to be kept securely).

3. Where an Australian government agency provides personal information to an overseas recipient to perform a service on its behalf, APP 8.1 and section 16C will operate to ensure that a data breach by the overseas recipient will be treated as having been an act by that Australian government agency unless an exception under APP 8.2 applies.

4. Under APP 5, an APP entity is required (if reasonable in the circumstance) to notify an individual or ensure that the individual is aware of whether that entity is likely to disclose personal information to overseas recipients (APP 5.2(i)). If the APP entity is likely to disclose the personal information to overseas recipients, the APP entity should specify the countries in which such recipients are likely to be located (if it is practicable to specify those countries in the notification), or otherwise make the individual aware of them (APP 5.2(j)).