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

Group: 2

Program: Other agency

Question No. AE15/046

Senator Dastyari asked the following written question from the 24 February and 27 March 2015 hearings:

From 12 March 2014, the Australian Privacy Principles (APPs) replaced the National Privacy Principles and Information Privacy Principles and will apply to government agencies and private sector organisations with an annual turnover of $3 million or more.

1. When a business and a customer sign a Privacy Authority, do they sign one to cover their relationship, or do they need to sign a new one for each transaction?

2. Why the duplication? Would you describe this as an example of Red Tape?

3. What public consultation did the designers of the APP do before it went public?

4. What additional public consultation has the OAIC done since the APP came into effect last year?

5. Have you sought the input and feedback of major industry associations?

6. Do you receive complaints about the APP?

7. What is the nature of these complaints?

8. How many complaints do you receive?

9. Would the government consider changing the Privacy Authority to a 'relational' agreement, instead of requiring a new one for each transaction?

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

1. Consent for the purposes of the Privacy Act means 'express consent or implied consent' (s 6(1)). Express consent is given explicitly, either orally or in writing, while implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the entity. There is no explicit requirement that consent be in writing or for a Privacy Authority to be signed. The OAIC's APP guidelines provide guidance about when an individual will be considered to have consented.

   Where an entity chooses to rely on consent to permit the handling of personal information, one way the entity may seek to gain that consent is to ask the customer to sign a document that the individual consents to the information handling. Whether that consent is valid for the whole relationship between the entity and the customers, or whether a new one is needed for each transaction, will depend on the circumstances. The key issue is whether the consent remains valid.

2. Whether a signed Privacy Authority is required for subsequent transactions will depend on the circumstances, including the scope of the original Privacy Authority and whether the consent remains valid for the subsequent transaction.

   The APPs are principles-based law. This provides APP entities with the flexibility to tailor their personal information handling practices to their diverse needs and business models, and to the diverse needs of individuals. As such, specific requirements for obtaining consent, or whether consent is required, are highly dependent on the context in which the personal information is to be handled and are not prescribed in the APPs.

3. The Attorney-General's Department has policy responsibility for the Privacy Act and oversaw the development of the APPs.

   The Australian Privacy Principles originated from recommendations in a report of the Australian Law Reform Commission, *For your Information: Australian Privacy Law and Practice*, Report No 108, 2008. The ALRC report followed an extensive community consultation program.

   On 14 October 2009, the former government released a response to the ALRC's report, following public consultation in 2009.

   In June 2010, the former government released *Exposure Drafts of Australian Privacy Amendment Legislation* which reflected its response to the ALRC report. The Exposure Draft Legislation included draft APPs and credit reporting provisions. On 24 June 2010, the Senate referred the Exposure Draft Legislation to the Senate Finance and Public Administration Committee for inquiry and report. After a public consultation process as part of its inquiry, the Committee released its report on 15 June 2011.

   On 23 May 2012, the former government introduced the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Reform Bill) into the Australian Parliament. The Reform Bill reflected elements of the Government's first stage response to the ALRC Report.

   The Reform Bill was referred to both the House Standing Committee on Social Policy and Legal Affairs (House Committee) and the Senate Legal and Constitutional Affairs Legislation Committee (Senate Committee), for inquiry and report. The House Committee tabled its advisory report on 17 September 2012. The Senate Committee tabled its report on 25 September 2012.

   The former government tabled its response to the Senate Committee report on 22 November 2012.

4. The Information Commissioner published APP guidelines in February 2014 ahead of the commencement of privacy law reform. The APP guidelines are the primary guidance for entities in how to interpret and comply with the APPs. The APP guidelines represent the completion of a significant amount of collaborative work with external stakeholders, including from entities and peak bodies across different sectors.

   Following input and feedback from stakeholders throughout the first year of the new privacy laws, the OAIC published updates to the APP guidelines in April 2015. Changes have been made to clarify some aspects of the guidance and respond to issues such as the introduction of separate privacy legislation in the ACT.

The OAIC routinely consults with, and receives feedback from, Government agencies, private sector organisations and individuals on issues relating to privacy. This includes regularly liaising with representatives of entities and industry bodies, for example, through speaking engagements and panel discussions at industry conferences, meetings, and informal feedback channels.

In addition, the OAIC has undertaken a range of consultative processes on privacy guidance, such as:

- *Guide to securing personal information* which provides guidance on taking reasonable steps to protect personal information, as required by APP 11
- *Privacy regulatory action policy* which explains the range of powers the Commissioner has and the way in which those powers are used
- Chapters of the *Guide to privacy regulatory action* which supports the *Privacy regulatory action policy* and provides a more detailed explanation of how the OAIC will exercise its regulatory powers
- *Guide to conducting privacy impact assessments* which provides an overview of a process for undertaking a privacy impact assessment to assist in identifying the impact that a project might have on the privacy of individuals, and set out recommendations for managing, minimising or eliminating that impact
- *Privacy management framework* which provides guidance on steps that could be taken to meet ongoing compliance obligations under APP 1.2
- *Credit reporting 'know your rights' series* which outline how personal information can be handled in the Australian consumer credit reporting system
- *Privacy business resource: Credit reporting — information held beyond its retention period* which assists credit reporting bodies in complying with notification requirements of regarding the handling and destruction or de-identification of credit reporting information held beyond its retention period for the purpose of responding to a correction request or dispute
- *Business Resource: Sending Personal Information Overseas* which assists organisations to understand their APP obligations when sending personal information overseas
- *Business Resource: Direct marketing and the Privacy Act* which provides guidance to business about the interaction between the APP 7 and the *Spam Act 2003* and *Do Not Call Register Act 2006*
- *What should healthcare providers consider before taking a photo of a patient on a mobile phone?* topic guidance which considers the key privacy issues that arise for clinicians when taking and sharing patient photos, including how the APPs would apply.

5. Please see response to question 4.

6. The OAIC does not have specific mechanisms in place to receive complaints about the APPs. However, the Privacy Act provides a mechanism for handling complaints about breaches of the APPs.

   Under section 36 of the Privacy Act the OAIC can receive complaints from individuals about breaches of the APPs by a range of Australian Government agencies and private sector organisations (called APP entities). Complaints about a breach of the APPs by APP entities must be about acts and practices that have occurred since 12 March 2014.

7. Complaints about breaches of the APPs can cover a range of issues related to each of the APPs. In summary, this means that complaints cover issues arising from the collection, handling, holding, accessing and correction of personal information in a manner contrary to the APPs. The table included in question 8 below shows the number issues related to each APP across complaints received by the OAIC since the APPs came into force.

8. Between the 12 March 2014, when the APPs came into force, and 31 March 2015 the OAIC received 863 complaints with at least one APP issue.

   The table below shows the number issues related to each APP across those 863 complaints. The total is different because each complaint may raise a number of separate issues.

APP 6 - Use or Disclosure	405
APP 12 - Access to Personal Information	342
APP 11 - Security of Personal Information	181
APP 3 - Collection	153
APP 10 - Quality of Personal Information	95
APP 7 - Direct Marketing	90
APP 5 - Notification of Collection	29
APP 13 - Correction	19
APP 1 - Open and Transparent Management	11
APP 2 - Anonymity and Pseudonymity	8
APP 4 - Unsolicited Personal Information	2
APP 9 - Adoption of Government Related Identifiers	2

9. Please see response to question 1.