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

Program: 1.7

Question No. SBE15/044

Senator Ludlam asked the following question at the hearing on 20 October 2015:

Senator LUDLAM: Sorry for the musical chairs. I have a couple more questions on biometric capability and then I might get one or two in on data retention. I do not know whether it was you who got cut off midsentence, or me—
Mr Rice: I was just going to say: do you want me to continue my answer?
Senator LUDLAM: Yes. Could you just reboot from where you were.
Mr Rice: Sure. I was talking about generic use cases that we have explored with potential users of the system at the Commonwealth and state level—
Senator LUDLAM: In the interests of time, could you table some documentation that sets out those generic use cases for us, so that I can ask some other specific stuff. I suspect I am going to find it is useful, and I suspect that it is going to eat up the whole 15 minutes to do it well.
Mr Rice: We can take that on notice.
Senator LUDLAM: If you could, thanks—just your reference cases. I am particularly interested in the push and pull. I might come back to that and just get through a couple of questions very quickly. What categories of offences will this tool be used to investigate, and will there be any gravity-of-conduct thresholds like those we debated extensively in data retention? Will you be able to chase down a litterer, for example?

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

The National Facial Biometric Capability will enable agencies to participate in two distinct facial matching services, described below.

The *Face Verification Service* (FVS) will enable agencies to verify a person's identity by searching or matching their photo (on a one-to-one basis) against an image on one of their government records. The FVS will enable three distinct functions:

1. *Retrieve Facial Biometric* - This function will take a person's evidence of identity (EOI) document type, EOI document number (and optionally date of birth) in the request and return a response from the Holding Agency with a facial image and, if needed and authorised, biographic details from the person's corresponding record.

   This could be used by a law enforcement agency to confirm that an EOI document presented by a person is not fraudulent (i.e. that the document does not contain a substituted photo with otherwise 'legitimate' biographical information of another person).

2. *Search Subject Request* - This function will take a person's first name, last name, date of birth and facial image in the request and return a response from the Holding Agency with the facial image from the person's corresponding record. In the event that there is more than one corresponding record with the same first name, last name and date of birth, the response will only indicate that there are multiple records.

This could be used by a law enforcement agency to confirm, in the absence of an EOI document, that the claimed identity of a person who is suspected to have committed a criminal offence matches that on one of their government records.

3. *Verify Subject Request* - This function will take a person's EOI document type, EOI document number and facial image (and optionally date of birth) in the request and return a simple 'Match' or 'No Match' response from the Holding Agency indicating whether there was a biometric match (based on an agreed threshold) against the person's corresponding record.

   This could be used, for example, where a person provides a driver's licence as evidence of their identity to apply for a passport. The FVS could enable the passport office, on a risk management basis, to ask the road agency to confirm that the photo on the application matches the photo held on their record.

The *Face Identification Service* (FIS) will enable agencies to match a photo of an unknown person against multiple government records (on a one-to-many basis) to help establish their real identity, or to detect where a person may hold multiple fraudulent identities.

The FIS will enable two distinct functions:

1. *Identify Subject Request* - This function will take a facial image and *mandatory* demographic details (age range and gender) in the request, and return a response from the Holding Agency with the most likely image match or matches (based on a pre-configured threshold/s) and, if needed and authorised, associated biographic data.

   This could be used, for example, where a law enforcement agency arrests a member of a child exploitation ring and seizes a number of computers that contain child exploitation material, including images of a suspected offender. The agency could submit a facial image and demographic details of the suspect and seek to match it against one or more government identity holdings (e.g. passports and/or driver licences) to establish their identity.

2. *Advance Identify Subject Request* - This function will take a facial image and *optional* demographic and/or partial biographic details in the request, and return a response from the Holding Agency with the most likely image match or matches (based on a pre-configured threshold/s) and, if needed and authorised, associated biographic data.

   This could be used, for example, where a terrorist cell has bombed a metropolitan office building and has threatened further attacks. A CCTV has captured the facial image of one of the suspected terrorists performing reconnaissance on the office building two days earlier. A specialist counter-terrorism team could submit the facial image to seek a match against several government identity holdings (e.g. passports, visas and driver licences) to determine the suspect's identity.

The Department is adopting a multi-faceted approach to promoting privacy in the design and operation of these services, informed by independent privacy impact assessments (PIA). The system utilises a 'hub-and-spoke' model which allows participating agencies to securely share their data through encrypted channels without creating a centralised database. A preliminary PIA on the hub and spoke design of the system has been completed and supports this approach.

A range of further PIAs will also be conducted to analyse information sharing arrangements between specific agencies. The next of these assessments is now underway, covering information sharing amongst an initial group of Commonwealth agencies that will participate in the FVS. Other PIAs will follow, on both the FVS and FIS, including those covering information sharing involving state and territory agencies.

Informed by these PIAs, privacy safeguards being implemented in the services include: limiting sharing to where agencies have confirmed a lawful basis (e.g. law enforcement purpose or consent based); formal data sharing agreements between agencies; a security and access model so that access to the Hub is controlled and transactions are auditable; strictly limiting access to the FIS to personnel with specialist training to guard against false matches; annual audits of agencies' use of the services; and monitoring use of personal information by oversight bodies, as already occurs.

The response to the honourable Senator's remaining question can be found in the Hansard transcript of 20 October 2015 on pages 124 to 125.