

**INQUIRY INTO ROAD TRANSPORT AMENDMENT
(NATIONAL FACIAL BIOMETRIC MATCHING
CAPABILITY) BILL 2018**

Organisation: NSW Government
Date Received: 5 November 2018

Standing Committee on Law and Justice Inquiry into the Provisions of the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 – NSW Government agency submission

Introduction

NSW Government welcomes the opportunity to lodge a submission for the Committee's consideration. The passage of the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 (the Bill) is an important step in fulfilling NSW's obligations under the Intergovernmental Agreement on Identity Matching Services (IGA) signed by first Ministers including the NSW Premier in October 2017. In signing the IGA, the Premier committed on behalf of NSW to endeavour to legislate to give effect to the transfer of driver licence images. This submission has been prepared at officer level and seeks to address the issues raised by the Legislative Review Committee in its 23 October report.

National Facial Biometric Matching Capability (the Capability)

The Capability enables authorised government agencies ('Participants'; law enforcement and road agencies) to verify or identify individuals for specific and limited purposes by searching databases of images taken for and used on official government records, such as driver licences and passports to find images and associated personal information of those individuals. Law enforcement agencies will be able to use the Capability's Facial Identification Service (FIS) for a limited number of defined purposes, including protective and national security, community safety and general law enforcement. Other authorised government agencies (for example, road agencies) will be able to use the Capability's 'Facial Verification Service' (FVS) to verify the identities of people they deal with, for example, with the person's consent when he or she is seeking a new driver licence, and without consent in limited circumstances, such as to ensure an individual is not seeking multiple licences in multiple names.

Authorised government agencies that contribute their images and associated personal information retain control over which, if any, other authorised government agencies (whether within their own jurisdictions, or from other jurisdictions) can access those images and that information, and to what extent. However, when using the FIS for 'general law enforcement' purposes, law enforcement agencies of one jurisdiction will only be able to search the images and associated personal information of other jurisdictions where the investigation concerns an offence carrying a maximum penalty of not less than three years' imprisonment. The Capability uses facial recognition technology to streamline existing manual and resource intensive processes and will speed up investigations.

Example of use

Example A – a person applies to provide private security at a sporting final.

- To verify that the person is who he/she asserts to be, the person provides his/her photo and details as stated on an official government record, such as a passport.
- The person consents for his/her image and information to be used by the Capability to verify his or her identity.
- These details are run through the FVS; if a direct match is found, this will verify the person's identity.

Example B – NSW Police surveillance identify an individual acting suspiciously by placing multiple unidentified objects in public bins around several stadiums, who they consider may pose a threat to national security.

- Using a still photograph from CCTV footage, a NSW Police Officer can run the person's face through the Capability's Facial Identification Service to generate potential matches for the purpose of conducting investigations into Australia's security.
- The NSW Police can then use the potential match results as an investigative lead to bring a potential suspect in for questioning.

Legislation

The Bill amends the *Road Transport Act 2013* (the RT Act) so that an 'authorised government agency' may upload and download photographs and associated personal information (e.g. the name of the person in the photograph) to and from the Capability. Participants in the Capability are all required to comply with the privacy laws of their home jurisdiction. At this stage, the only NSW government agency that will be uploading images and associated personal information is Roads and Maritime Services (RMS).

'Authorised government agencies'

In order to be able to access the Capability, all government agencies must satisfy a number of legislative, procedural and administrative criteria. The Capability can only be accessed or used by government agencies that:

- have a legislative basis upon which they can have access to the Capability;
- are 'authorised'; and
- have a lawful purpose for each instance of use.

The amendments to the RT Act in this Bill will provide the legislative basis upon which RMS can upload its images and associated personal information to the Capability, and upon which RMS, and, as may be necessary in future, other government agencies operating as RMS's agent, such as Service NSW, may seek authorisation to use the Capability to conduct verification and identification searches.

To be authorised to access the Capability, an agency with a legislative basis for use must execute a Participation Agreement with the Capability's host, currently the Commonwealth Department of Home Affairs. The Participation Agreement is a contract between the Capability host and each other agency with access to the Capability (to upload images, download images, or both). The Participation Agreement sets out:

- all agencies' roles, rights, responsibilities and obligations;
- strict conditions for use, including what training, compliance, security and audit standards each agency must meet; and
- the framework within which agencies must negotiate their data sharing and access arrangements and conditions in accordance with required privacy and security safeguards.

After executing a Participation Agreement, an agency must then execute Participation Access Arrangements with each other government agency whose data the first agency wishes to access via the Capability. For example, RMS would need to execute Participation Access Arrangements with

each other jurisdiction's road agencies in order to access other jurisdictions' driver licence images and associated personal information.

A Government agency that hold images and associated personal information can elect *not* to execute Participant Access Arrangements with any other agency (whether within its own jurisdiction or elsewhere) if it is not satisfied that the other relevant agency has the legislative basis, the legitimate need, or the necessary security or audit safeguards in place to justify that access. A Government agency can also provide restricted access, by limiting which of its images and information can be accessed and under what conditions.

'Agencies and their Agents'

RMS's customer service functions (including issuing driver licences and registering vehicles) are carried out by Service NSW as its delegate. The reference to 'agent' in the Bill is intended to capture Service NSW when it performs RMS functions in the event that verification of customer identity should occur in real time when the customer is transacting at a Service Centre.

'Lawful purpose' or 'functions' to keep and use photographs and personal information obtained from the Capability

A 'lawful purpose' of an agency is the carrying out of a function of the agency according to law. Government agencies only have the functions given to them under statute. The Bill limits an agency's use of information to those lawful purposes and therefore prohibits use of the Capability for any other purposes.

RMS's main statutory functions are driver licensing, vehicle registration, maritime licensing, vessel registration, licensing of driver instructors, issue of bus driver authorities and issue of mobility parking permits. Since the Bill may apply to agencies other than RMS, where executing RMS's functions on its behalf, the Bill refers to the lawful purposes of 'agencies' generally.

Privacy

The Capability enables authorised government agencies to verify or identify individuals by matching their facial images with images on official records, such as driver licences or passports, accessible through the Capability. Verification of a person's identity will only occur with the person's consent or as authorised by law. Identification of an unknown person can only occur for specific, limited purposes, principally law enforcement and national security. The Capability does not provide automated or 'real time' surveillance of public spaces.

The system has been designed with robust privacy safeguards in mind.

- Each agency authorised to use the identity matching services will be bound by strict conditions about their use of the Capability.
- In NSW, the *Privacy and Personal Information Protection Act 1998 (PPIPA)* will continue to apply, with the exclusion of ss 9 and 10.
- The Capability has strict authorisation, audit and training requirements; an established compliance framework to identify and manage any misuse; and clear conditions on the parameters of permissible use of the different services within the Capability.
- NSW data would not be available to the private sector without the prior approval of the NSW Government.

Ensuring customers are properly informed

RMS will update its existing Privacy Statements to inform their customers that their images may be uploaded to the Capability.

The Department of Home Affairs (DHA) proposes an educational campaign to inform citizens about the Capability. The following information is already available to the public via the DHA website (www.homeaffairs.gov.au/about/crime/identity-security/face-matching-services):

‘The system will adopt best practice security and access arrangements in accordance with the Commonwealth Government’s Protective Security Policy Framework and the Information Security Manual, and will be subjected to independent penetration and vulnerability tests as well as an independent security review by the Australian Signals Directorate.’

Exemption from Section 9 of the *Privacy and Personal Information Protection Act (PPIPA) 1998*

RMS will use the Capability to compare photographs of customers with images held in the Capability in order to verify their identities, detect fraud and ensure that a driver only holds one driver licence in Australia.

Section 9 of the PPIPA provides that a public sector agency must collect personal information directly from the relevant individual unless the individual consents otherwise. The Bill proposes that section 9 of the PPIPA will not apply in relation to any photographs or personal information downloaded by the agency from the Capability. This is proposed in a new section 271A (3).

The nature of the Capability (that is, the centralised storage and matching of images from around Australia, including driver licence, passport and citizenship certification photos) would make it impossible for RMS to comply with section 9.

Exemption from Section 10 of the *Privacy and Personal Information Protection Act (PPIPA) 1998*

Section 10 states that an Agency must take *such steps as are reasonable in the circumstances* to provide customers with what is commonly known as a privacy statement or personal information collection notice providing information about the collection of information.

The Bill proposes that section 10 of the PPIPA will not apply in relation to any photographs or personal information downloaded by the agency. This is proposed in a new section 271A (3). Compliance with section 10 is not possible where images are uploaded to the Capability rather than being directly collected by the Agency from the individual concerned.

Nevertheless, RMS proposes to update its Privacy Statements to inform customers about RMS’ participation in the Capability.