Charles Sturt University

Dr MARCUS SMITH

CENTRE for LAW and JUSTICE

6 September 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Department of the House of Representatives
PO Box 6021
Parliament House
Canberra ACT 2600

By email: pjcis@aph.gov.au

Dear Committee Secretary,

Review of the Identity-matching Services Bill 2019

1. Background

1.1 I am a legal academic with a research interest in regulatory issues associated with biometric identification.[1] I thank the Committee for the invitation to make a submission to this Review and hope it is of assistance in making recommendations. I would be happy to answer any questions the Committee may have in relation to this submission.

1.2 This bill provides a legislative basis for implementing measures contained in the *Intergovernmental Agreement on Identity Matching Services* (IGA), agreed by COAG in October 2017. The IGA seeks to facilitate the exchange of identity information through automated facial recognition technology (AFRT) to help prevent crime and promote law enforcement and community safety objectives.

1.3 The Identity-matching Services Bill 2019 (IMS Bill) authorises the Department of Home Affairs to develop, operate and maintain: an 'interoperability hub' through which participating agencies and organisations can request and transmit information; and the

[1] See e.g. Smith, M., Mann, M. and Urbas, G. (2018). *Biometrics, Crime, and Security,* Routledge, Abingdon, United Kingdom; Mann, M. and Smith, M. (2017). 'Automated Facial Recognition Technology: Recent Developments and Regulatory Options' 40(1) *University of New South Wales Law Journal* 121.

National Driver Licence Facial Recognition Service (NDLRFS), a federated database of information contained in government identity documents such as driver licences.

1.4 The IMS Bill establishes identity-matching services that will operate through the hub. These include the Face Verification Service (FVS), enabling the identity of a specific person to be verified; and the Face Identification Service (FIS), enabling digital matching of a facial image with images of one or more people, in order to identify a person.

2. Automated Facial Recognition Technology

2.1 AFRT involves the automated extraction, digitisation and comparison of the spatial and geometric distribution of facial features. Using a digital photograph of a subject's face, a contour map of the position of facial features is converted into a digital template using an algorithm.[2] It uses an algorithm similar to that used in fingerprint recognition to compare an image of a face with one stored in a database.[3]

2.2 Compared with other forms of biometrics, such as DNA and fingerprint identification, AFRT can use existing information, such as photographs and can be conducted from a distance. Open source images can be collected from social media, or the internet more broadly, and integrated into AFRT systems.[4] AFRT can also be linked with closed circuit television systems that currently exist in public and private spaces.[5]

2.3 Compared with other biometric identity repositories available for searching in Australia, the proposed approach to matching facial images will be much larger in scope. An estimate can be made based on currently available data. For example, New South Wales Roads and Maritime Services data indicates that there are 5.5 million drivers' licences in NSW.[6] The total population of NSW is 7.9 million,[7] indicating 70 percent have a drivers licence. If this rate is reflected nationally, approximately 17 million Australian's would hold a drivers licence. When the number of Australians who hold a passport but not a driver licence is added to this figure, the number would rise further. Passport holders would include a significant number of Australians under the age of 18, and there would also be a significant

---

[2] Ricanek K and Boehnen, C. 'Facial Analytics: From Big Data to Law Enforcement' (2012) 45(9) *Computer* 95.
[3] Adler, A and Schuckers, M. 'Comparing Human and Automatic Face Recognition Performance' (2007) 37 *IEEE Transactions on Systems*, *Man, and Cybernetics, Part B: Cybernetics* 1248.
[4] Stone, Z, Zickler, T, and Darrell, T. 'Toward Large-Scale Face Recognition Using Social Network Context' (2010) 98 Proceedings of the IEEE 1408.
[5] Gates, K. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York University Press, 2011)
[6] NSW Roads and Maritime Services, *Licencing*. Available at: http://www.rms.nsw.gov.au/cgi-bin/index.cgi?fuseaction=statstables.show&cat=Licensing
[7] Australian Demographic Statistics, *Population Data December 2017*. Available at http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0

number of 16 and 17 year old Australians with provisional drivers licences or learners permits.

2.4 Other biometric identification repositories that currently exist in Australia include the National Automated Fingerprint Identification System (NAFIS) and the National Criminal Investigation DNA Database (NCIDD). These are operated by the Australian Criminal Intelligence Commission (ACIC) and are much smaller in scope. Inclusion in these systems is limited to individuals who have had contact with law enforcement investigations. DNA profiles are uploaded to the database by state police agencies or the AFP. [8]

2.5 The NCIDD was established in 2001 via an amendment to the *Crimes Act 1914* (Cth). A person's DNA profile is only included in the NCIDD if they have been convicted of a criminal offence, or in the case of suspects, for a defined period of time, such as 12 months.[9] The NCIDD currently contains approximately 800 000 DNA profiles.[10]

2.6 In contrast with existing biometric databases, the IMS Bill appears to provide for an 'interoperability hub' where the facial images remain with the states (or in the case of passport images, the Department of Foreign Affairs and Trade), however, the hub could still be searched as though the images were held in a Commonwealth database. This approach may, for practical purposes, have the same effect as if the data were held by the Commonwealth. It is unclear why this approach has been adopted.

3. Balancing Security and Privacy

3.1 The Government should make use of the best available technology in providing security for the community. However, any approach should be proportionate and targeted. In determining this, the mechanisms that exist to independently oversight the proposed capabilities will be important.

3.2 The Office of the Australian Information Commissioner (OAIC) and its state and territory equivalents have broad authority in the area of biometric information. Biometric information is complex, used by law enforcement and security agencies in various ways, and the relevant technologies continue to develop. It is unclear whether the OAIC has the resources and specialist knowledge of biometrics to provide effective oversight of new developments such as the one proposed in these Bills. At present in Australia, no

[8] Smith, M., Mann, M. and Urbas, G. (2018). *Biometrics, Crime, and Security,* Routledge, Abingdon, United Kingdom
[9] Smith, M. DN*A Evidence in the Australian Legal System* (LexisNexis Butterworths, 2016).
[10] Australian Criminal Intelligence Commission, *National Criminal Investigation DNA Database*. Available at: https://www.acic.gov.au/our-services/biometric-matching/national-criminal-investigation-dna-database

independent, specific oversight mechanisms exist to oversee or regulate the collection, retention and use of biometric information.

3.3 In overseas jurisdictions, independent statutory commissioners have been appointed and demonstrated a capacity to respond to concerns relating to consent, retention and use of biometric information. For example, the United Kingdom has created a Commissioner for the Retention and Use of Biometric Material (UK Biometrics Commissioner). The UK Biometrics Commissioner was established under the *Protection of Freedoms Act 2012* (UK) in response to the judgement in the *S and Marper v United Kingdom*[11] case in the European Court of Human Rights in 2008. The mandate of the UK Biometrics Commissioner is to regulate the use of biometric information and provide a degree of protection from disproportionate law enforcement action.[12]

3.4 The UK Biometrics Commissioner has statutory powers that include oversight of the retention of biometric information by deciding on applications made by police to retain biometric information, as well as reporting to the Home Secretary about these functions or other matters considered appropriate. The UK Biometrics Commissioner's powers do not presently extend to biometric information other than DNA or fingerprints.[13] However, the House of Commons Science and Technology Committee has recommended that the statutory responsibilities of the Biometrics Commissioner 'be extended to cover, at a minimum, the police use and retention of facial images'.[14]

4. Summary

4.1 The capability proposed by these bills is a significant development enabling the extraction and digitisation of biometric information from routinely collected and readily available photographs, facilitating information sharing and integration. It may be expected that with ongoing developments in technology, opportunities to use this data will expand and information sharing will become more efficient. There is a need to consider the adequacy of existing independent oversight mechanisms in light of new technologies and the scope of the present proposal.

4.2 The Biometrics Commissioner model that has been adopted in the UK, with additional powers in relation to biometric facial images, would provide appropriate independent oversight of the developments proposed by these bills, and more broadly. It would be an

[11] [2008] ECHR 1581.
[12] *Protection of Freedoms Act 2012* (UK) c 9, s 20.
[13] Office of the Biometrics Commissioner, *About Us*. Available at: https://www.gov.uk/government/organisations/biometrics-commissioner/about
[14] House of Commons Science and Technology Committee, Parliament of the United Kingdom, *Current and Future Uses of Biometric Data and Technologies* (2015) 34.

important step towards ensuring that there is a reasonable and proportionate balance between the need to use available new technology to protect the community from harm, and maintain appropriate standards regarding individual rights.