MONASH University

Committee Secretary,
Parliamentary Joint Committee on Intelligence and Security,
PO Box 6021,
Parliament House,
Canberra, ACT 2600.

email: pjcis@aph.gov.au

2 October 2018

Re: Identity-matching Services Bill 2018

Dear Committee Chair,

Thank you for the opportunity to submit a late submission to the review into the Identity-matching Services Bill 2018.

I make this submission based on my professional and research expertise. I am a legal academic, holding the position of Professor of Criminal Jurisprudence at Monash University, having been based previously in the UK. I have written numerous peer-reviewed academic articles and a book on forensic and biometric databases, looking in particular at the human rights implications of such investigative and policing tools in a comparative context.[1] Since 2017 I have been an appointed member of the UK Home Office Biometrics and Forensics Ethics Group, and I continue in that role currently.

While I do not dispute the benefit of identity-matching services for state agencies for the purposes of security and policing, it is imperative, both legally and normatively, for any such services to be defined precisely, and for these to be bounded by adequate safeguards. As the Bill stands, such clear definitions and safeguards are lacking. As such, I cannot condone passing of the Identity-matching Services Bill 2018.

Here I express, in brief, some concerns about the draft Bill, framed around five main issues: the right to privacy; the right not to be discriminated against; the precision of drafting; governance and oversight; and reliability of the technology.

1. The right to privacy

The services and hub outlined in the Bill impact significantly on the right to privacy, as protected by Article 17 of the International Covenant on Civil and Political Rights. Essentially, the Bill enables the collection, storage, processing, and sharing of sensitive biometric information of individuals who have not been convicted of any criminal offence; indeed they need not be suspected of any offence. In the European context, permanent

[1]
- "Privacy, Crime Control and Police use of Automated Facial Recognition Technology" (2018, under consideration by *Criminal Law Review*) (with Purshouse, J.)
- *The Collection and Retention of DNA from Suspects in New Zealand* w/ Lynch, N. (Victoria University Press, 2015)
- "'To Have and To Have Not': The Retention of DNA for Criminal Justice Purposes in New Zealand" [2016] *New Zealand Law Review 319-356* (with Lynch, N.)
- "Competing Paradigms? The Use of DNA Powers in Youth Justice" (2012) 12 Youth Justice 3-18 (with Lynch, N.)
- "'Non-Conviction' DNA Databases in the USA and England: Historical Differences, Current Convergences" (2011) 15 *International Journal of Evidence and Proof* 281-310
- "'Non-Conviction' DNA Databases and Criminal Justice: A Comparative Analysis" (2011) 1 *Journal of Commonwealth Criminal Law* 55-77
- "A Rights-Based Analysis of DNA Retention: 'Non-Conviction' Databases and the Liberal State" (2010) 12 *Criminal Law Review* 889-906
- "DNA Databases and Innocent Persons: Lessons from Scotland?" (2010) 4 *Juridical Review* 285-297

Faculty of Law
15 Ancora Imparo Way, Clayton, VIC 3800

retention of biometric material in such non-conviction based databases has been found to breach the right to privacy and family life as provide for in Article 8 of the European Convention on Human Rights (*S v Marper* (2009) 48 EHRR 50). Ultimately, any encroachment on the right to privacy should be necessary and proportionate. The effect of the Bill on the right to privacy is disproportionate, and numerous elements of it are unnecessary.

Individuals are entitled to know why and for what purpose(s) their personal information is collected and stored. The Bill breaches this, in permitting the Department to "use or disclose for any of those purposes information so collected (regardless of the purpose for which it was collected)" (section 3). This is both unnecessary and disproportionate in its impact on the right to privacy, and breaches the consent given by individual to having their personal information collected and used for a particular purpose.

Moreover, the breach of the right to privacy is compounded by the possibility of non-government entities accessing the identity matching services (see section 7 and 10). These enabling provisions must be deleted from the Bill.

If the Bill proceeds, in seeking to mitigate the effect on the right to privacy, 'identification information' should only be defined in the Bill (section 5), and power to do so should not be delegated to the Minister.

2. The right not to be discriminated against

Facial recognition and identity matching technology has the potential to threaten an individual's right to be free from discrimination, as protected by Article 2 of the ICCPR. This may occur in two separate ways. First, state agencies may deploy the technologies in a distinct way against different demographic groups, whether intentionally, through bias, or otherwise. Secondly, existing research into identity matching technology indicates that ethnic minorities and women are misidentified at higher rates than the rest of the population (Buolamwini and Gebru, 2018; Klare et al, 2012). This relative inaccuracy may lead to members of some groups being misidentified and so their data being retained and their being subject to coercive policing or security measures inappropriately.

3. Precision of drafting

Throughout, the Bill is broadly drafted, and it provides for a great deal of discretion. I suggest that more precise drafting is vital, both to avoid ambiguity and to ensure adequate safeguards for individuals. Section 6, for instance, refers to the prevention of crime, community safety, and road safety. If the Bill is retained, I suggest that section 6(3) should pertain to the prevention of a limited range of serious offences only. I urge the Committee to recommend deletion of section 6(7) and (8).

4. Governance and oversight

The proposed scheme of governance and oversight in the Bill is inadequate, in not extending beyond an annual report to the Minister to be tabled in Parliament. The use of and access to biometric databases should be reviewed annually from a human rights and ethical standpoint, and the annual report should include details of errors and breaches. In a broader governance sense, I suggest consideration should be given to the scheme adopted in the UK for more thorough oversight. While this UK model is not absolutely ideal in terms of its complexity and degree of overlap of powers/remit (see the co-existence of the Biometrics and Forensics Ethics group, the Forensic Science Regulator, the Information Commissioner, and the Biometrics Commissioner), it provides a helpful prototype for construction of an oversight scheme.

5. Reliability of the technology

Facial recognition/identity matching is a nascent technology, and there are significant concerns about the

MONASH University

reliability or otherwise of its algorithms and the biases that can be inherent in them. Experience from the UK exemplifies this. South Wales Police is the national lead on facial recognition technology and received a £2.6 million UK Government grant to run a pilot scheme. SWP deployed the system of a private company called Neoface at 18 public gatherings between May 2017 and March 2018, after which concerns were raised about accuracy: "91% of matches—2,451—incorrectly identified innocent members of the public" (Big Brother Watch, 2018).

Notably, there is no publically available indication of the measurement/standard which entails an identity "match", and this may differ depending on the service provider and the parameters of the algorithm. There is no indication in the Bill as to whether or how the level of accuracy at which a match is deemed "successful" will be set. A lower level of accuracy would, of course, ensure that the data of a larger cohort of people would be processed and shared.

I would be pleased to provide further detail on any of the above submissions, should that be of help to the Committee.

Yours faithfully,

Professor Liz Campbell

Faculty of Law
15 Ancora Imparo Way, Clayton, VIC 3800

edu