Human Rights Law Centre

Answers to questions on notice: Inquiry into the *Identity-matching Services Bill 2018* and the *Australian Passports Amendment (Identity-matching Services) Bill 2018*

29 August 2018

Question from Mr Leeser – What powers should be in legislation as opposed to subordinate legislation

As the Australian Human Rights Commission's submission to this inquiry sets out, a measure which interferes with the right to privacy should be prescribed by law and legislatively defined with sufficient precision to enable people to understand its operation in advance and plan their conduct accordingly.

As set out in our submission, and submissions like that of the Australian Human Rights Commission, the bill delegates broad powers to establish the scheme to the Secretary and is striking as to the complete absence of detail as to how the facial recognition scheme will operate. Details and safeguards referred to in the Intergovernmental Agreement do not even appear in the proposed legislation.

It is simply inappropriate for this detail to be left out of the legislation, more so given the novelty of the proposed scheme and the serious risks involved. How the scheme operates requires careful scrutiny, full transparency and utmost certainty and must have the appropriate safeguards in place before it is enabled by Parliament.

Further, the bill would grant broad powers to the Minister to make rules:

- defining new forms of identification information (which could include DNA data or health records) that could be accessed through the scheme; and
- adding new identification services to the scheme.

Whether or not the technological capability currently exists, we note that the current definition of a Facial Information Service in the bill is arguably broad enough to allow the supply of real-time or almost real-time CCTV footage into the system to identity people from images contained in the database. If there is doubt, or if the Minister wanted to add other identification services, they could do so under the rule making power.

Again, it is simply inappropriate for these broad powers to be given to the Minister. Proposals to expand the scheme by adding new forms of information or new identification services should be set out in proposed amending legislation and subject to full Parliamentary and public scrutiny as opposed to the diminished scrutiny exercised over subordinate legislation.

Question from Senator Fawcett – Use of facial recognition technology in crowds to prevent serious crime

Senator Fawcett asked whether facial recognition technology should be used by law enforcement agencies to scan a crowd at a gathering or protest to identify people known to be highly disruptive and violent to enable preventative measures.

The UN Special Rapporteur on the rights to freedom of association and assembly in 2016 published a joint report on "The Proper Management of Assemblies" which provides helpful guidance in assessing when facial recognition technology is justified at protests or other gatherings.[1] The report provides that:

- Legislation and policies regulating the collection and processing of information relating to assemblies or their organizers and participants must incorporate legality, necessity and proportionality tests. Given the intrusiveness of such methods, the threshold for these tests is especially high.
- States should implement robust and appropriate protections of public privacy and safety prior to the adoption of any biometric technologies, including facial recognition software, in the context of assemblies.
- The public should be notified when they are, or may be, recorded during an assembly.
- Recording peaceful assembly participants in a context and manner that intimidates or harasses is an impermissible interference with rights.
- States should develop and implement laws and policies requiring that personal information may be collected or retained only for a lawful, legitimate law enforcement purpose. Such information should be destroyed after a reasonable time period set out in law.
- States should put in place mechanisms whereby individuals can ascertain whether and, if so, what information has been stored, and be provided with access to an effective process for making complaints relating to the collection, retention and use of their personal information and that can lead to rectification or expungement.
- Intrusive pre-emptive measures should not be used unless a clear and present danger of imminent violence actually exists.

Applying these tests to any particular situation will require analysis of issues including:

- The threat that law enforcement agencies are responding to. How serious is it? Is there specific information that a serious offence is planned or imminent or are agencies merely worried about low level disruptive conduct that might occur?
- What likely impact will the facial recognition surveillance have on attendees, bearing in mind the high risk of false matches, particularly for ethnic minorities?
- Can the use of the facial recognition technology be limited or targeted to address the specific serious risk?
- Are there other ways to manage the risk without the use of facial recognition technology?

Questions from Mr Dreyfus – Purpose behind police use of facial recognition technology on protesters at arms fair in South Wales and at the Notting Hill Carnival.

[1] Maina Kiai and Christof Heyns, Joint Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the Proper Management of Assemblies, 31st sess, UN Doc A/HRC/31/66 (February 2016)

Human Rights Law Centre

UK police used the facial recognition technology at the Notting Hill Carnival reportedly to identify wanted people who had offended and people whose bail conditions preventing them from attending such an event. Information on the reported purpose and the extremely high inaccuracy rate of the technology is set out in Big Brother Watch's 2018 report.[2]

It is not clear why South Wales police were using facial recognition technology at a protest outside an arms fair. The incident was reported in the media, noted in the Big Brother Watch report referred to above and criticised by the UN Special Rapporteur on the right to privacy (see: https://www.theguardian.com/world/2018/jun/29/un-privacy-chief-criticises-use-of-facial-recognition-in-wales).

[2] Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018), available at https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf