Law Council
OF AUSTRALIA

Review of the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019

Parliamentary Joint Committee on Intelligence and Security

2 October 2019

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2019 Executive as at 14 September 2019 are:

- Mr Arthur Moses SC, President
- Ms Pauline Wright, President-Elect
- Dr Jacoba Brasch, Treasurer
- Mr Tass Liveris, Executive Member
- Mr Ross Drinnan, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council is grateful for the assistance of the Privacy Law Committee and Media and Communications Committee of the Business Law Section and its National Criminal Law Committee in the preparation of this submission.

Executive Summary

1. The Law Council welcomes the opportunity to provide this further submission to the Parliamentary Joint Committee on Security and Intelligence's (**Committee**) review of the Identity-Matching Services Bill 2019 (Cth) (**IMS Bill**) and the Australian Passports Amendment (Identity-matching Services) Bill 2019 (Cth).

2. The Law Council provided a submission and supplementary submission to the Committee's review into the Identity-matching Services Bill 2018 (Cth) and the Australian Passports Amendment (Identity-matching services) Bill 2018 (Cth) (**2018 Bills**).[1] The Law Council also provided evidence to the Committee at its hearing on 3 May 2018. The Law Council thanks the Committee for accepting this previous contribution as evidence for the current review.

3. The specific issues already raised by the Law Council in 2018 are reiterated in this submission, as are the specific recommendations for technical reform. Some of the key concerns raised by the Law Council regarding the facial recognition capabilities of the identity-matching services proposed by the IMS Bill are:

    (a) the effectiveness of the technology to correctly identify individuals and the adverse impact on privacy from false matches;

    (b) the undermining of the notion of informed consent;

    (c) the potential for individuals to be targeted based on their membership of a particular race, ethnic group or religion;

    (d) the privacy safeguards referred to in the *Intergovernmental Agreement of Identity Matching Services* (**Intergovernmental Agreement**) are not reflected in the IMS Bill; and

    (e) weaknesses in oversight and accountability measures.

4. A key purpose of this submission is to highlight that the increase in the use of closed-circuit television (**CCTV**) with facial recognition technology in both public and semi-public spaces around Australia, such as streets, parks, stadiums and transport hubs, heightens the requirement for the IMS Bill to include appropriate, legislated boundaries for reasonable and proportionate use of identity-matching services and effective and independent oversight.

5. Provision of an 'interoperability hub' as a 'hub' should not absolve the operator of that hub from responsibility to ensure that users of the hub, including the requesting agency and the data holding agency, make only reasonable and proportionate use of the hub. The hub is a powerful new capability, not just an extension of past non-image practice (i.e. fingerprint matching). Provision of this powerful capability requires effective and independent oversight of how and when participating agencies, entities

[1] Law Council of Australia, Submission No 8 to the Parliamentary Joint Committee on Intelligence and Security, *Review into the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018* (21 March 2018) <https://www.aph.gov.au/DocumentStore.ashx?id=de0b7e90-2ada-41e0-a246-3786a2ad423a&subId=564484>; Law Council of Australia, Submission No 8.1 to the Parliamentary Joint Committee on Intelligence and Security, *Review into the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018* (6 April 2018) <https://www.aph.gov.au/DocumentStore.ashx?id=c33c5dc4-f053-42fe-be12-485803467f80&subId=564484>.

and organisations (**participating agencies**)[2] are permissioned to use the hub and to ensure that uses of the hub do not circumvent relevant restrictions.

6. This submission focuses on the appropriate balance that must be struck providing flexibility for growth of the services in the future and adequate scrutiny of that growth, as well as independent oversight of the Department of Home Affairs' (**Department**) operation of the interoperability hub[3] and adequate transparency of its use by participating agencies.

7. This submission also details the use of automated facial recognition technology in the United Kingdom (**UK**). The Law Council considers that the UK experience with the use of automated facial recognition technology may provide the Committee with examples of the risks and challenges associated with the use of facial recognition technology. Australia's absence of similar human rights and data protection frameworks that exist in the UK reinforces the need for the IMS Bill to legislate boundaries for reasonable and proportionate use of identity-matching services and robust safeguards, oversight and transparency measures.

8. Additionally, this submission also notes the initiatives of the European Commission in relation to the development of trustworthy artificial intelligence (**AI**) in the European Union (**EU**) and refers the Committee to the Law Council's recommendations for an Australian ethics framework for AI.[4]

Introduction

9. Capture and use of facial images of individuals through CCTV for the purpose of facial recognition is rapidly increasing in Australia. The Law Council considers that the uptake of this type of surveillance heightens the need for the IMS Bill to include appropriate, legislated boundaries of which there is robust and independent oversight.

10. The Law Council recognises that there often will be legitimate and proportionate public interest uses of facial recognition technology, such as to address identity crime and sharing information for the purposes of facilitating law enforcement, protecting Australia's national security and community safety. However, to assure that uses are reliably and verifiably legitimate and proportionate, controls and safeguards are reasonably required. Reasonable controls and safeguards do not undermine proper public interest uses, rather, they assure citizen trust in the system and thereby nurture ongoing legitimacy and therefore sustainability of the system. Like all systems, the system is only as trusted as its least legitimate known use: any misuse of the system by any participating authority is likely to undermine citizen trust in the system itself, and its operation. Media and citizens are not likely to closely allocate responsibility and fault if the system is perceived to allow misuse without adequate protection, early detection and prompt remediation.

11. The Law Council recognises that the identity-matching services that are proposed in the IMS Bill seek to establish processes within a framework for the sharing of identity information, including biometric data, between the Commonwealth, states and territories, which can be seen as somewhat of an improvement on the ad-hoc sharing

[2] See *National Facial Biometric Matching Capability, Face Matching Services – Services*, *The Department of Home Affairs and the Agency* (Template Memorandum of Understanding) 7, definition of 'participant'.
[3] Identity-Matching Services Bill 2019 (Cth) cl 14.
[4] Law Council of Australia, Submission to the Department of Industry, Innovation and Science, *Artificial Intelligence: Australia's Ethics Framework* (28 June 2019) <https://www.lawcouncil.asn.au/resources/submissions/artificial-intelligence-australias-ethics-framework>.

arrangements that currently exist between agencies, relying on manual processes which may not be secure and may be difficult to audit.[5]

12. However, it is critical to ensure that the legislation which enables the use of this type of technology does not permit a creep toward broad social surveillance in Australia. The Australian community has the right to have a secure and safe lifestyle without excessive oversight or interference with their individual private lives when, for example, attending sporting events, concerts or frequenting public areas and semi-public venues such as stadiums, airports, transport hubs and clubs.

13. Biometric information (as sensitive personal information) about individuals is rightly subject to a higher level of privacy protection than other personal information about individuals. Facial recognition fundamentally engages the right to privacy, as protected by Article 17 of the *International Covenant on Civil and Political Rights* (**ICCPR**).[6] Article 17 of the ICCPR states:

> *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks.*[7]

14. The right to privacy may comprise 'freedom from unwarranted and unreasonable intrusions into activities that society recognises as belonging to the realm of individual autonomy'.[8] The right to privacy is limited, but any incursions may not be 'arbitrary or unlawful'. To be lawful, any incursions must be precise and sufficiently circumscribed.[9] To avoid arbitrariness, the incursion must be proportionate to a legitimate objective under the ICCPR, necessary and reasonable in the circumstances.[10] The right to privacy applies, subject to these limitations, in all spheres of life.

15. Like all privacy rights, this right must sometimes give way to societal rights, including a right of other citizens to public safety. The Law Council does not contend that CCTV should not be used for public safety, including reasonable and controlled secondary use of images of individuals for public safety. Technology such as CCTV, when used responsibly, is important in order to enhance public safety. However, where sensitive personal information such as facial images are being matched to an individual's identity, controls and safeguards are required in order to ensure that there is appropriate balancing of the individual's right to privacy and the right of other citizens to public safety. In summary, sharing of an extensive amount of biometric data, for a broad range of purposes and to a broad range of agencies, may unduly impinge personal rights and liberties, particularly the right to privacy. The use of biometric technologies, including facial recognition technology, must therefore be tightly controlled.

---

[5] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) 47.
[6] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 993 UNTS (entered into force 3 January 1976)
[7] Ibid art 17.
[8] Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights* (3rd Edition, Oxford University Press, 2013), [16.01] citing SE Wilborn, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace', (1998) 32 *Georgia Law Review* 825, 833.
[9] Human Rights Committee, *General Comment No. 16*, 32nd session, UN Doc HRI/GEN/1/Rev.9 (Vol I), [8].
[10] Ibid 4.

16. The wide-spread use of identity matching services upon the vast majority of Australians must be justified as aimed at a legitimate objective and be reasonable and proportionate. The IMS Bill has been drafted through a lens of 'future proofing'.[11] While the Law Council recognises the need for legislative durability, the IMS Bill as currently drafted does not include partial checks and constraints against creep past the line of legitimate and proportionate uses of an interoperability hub to illegitimate and disproportionate uses. The IMS Bill leaves open the potential for:

    (a) local government and non-government organisations to access the Face Verification Service (**FVS**) with minimal or no detail contained in the IMS Bill about:

        (i) how consent would be obtained;

        (ii) what use the local government or non-government organisation intends to make of the data;

        (iii) what privacy protections would apply;

        (iv) how compliance with the law would be monitored; or

        (v) what private sector organisations access the FVS;[12]

    (b) the Face Identification Service (**FIS**) to be used for the detection, investigation or prosecution of minor offences because the IMS Bill does not contain the threshold that the offence must carry a maximum penalty of three years imprisonment, as is contained in the Intergovernmental Agreement;[13]

    (c) the proposed limits on the number of images presented for matching to a participating authority does not in practice limit the number of images requested to those numbers because multiple requests may be made by a participating authority around the putatively matched image; and

    (d) new types of identity information to be collected, used and shared by the interoperability hub if determined by the Minister through rules.[14]

Recommendations

17. To ensure that there are more clearly defined limits on the legitimate and proportionate use of identity-matching services proposed in the IMS Bill, as well as greater oversight and transparency, the Law Council recommends that the IMS Bill be amended to:

    (a) introduce the following safeguards for when the FVS is accessed by local government and non-government organisations:

        (i) notice to be given to individuals about the collection and use of their identifying information;

[11] Evidence to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 August 2018 (Andrew Rice, Assistant Secretary, Identity and Biometrics Division, Department of Home Affairs).
[12] Identity-Matching Services Bill 2019 (Cth) cl 7.
[13] Ibid cl 6(3).
[14] Ibid cl 5(1)(n).

(ii) penalties for private organisations if they use the interoperability hub or identity data in an unauthorised way;

(iii) mandatory training of empowered individuals within local government or non-government organisation about permitted uses; and

(iv) information be provided by the local government or non-government organisation about the use of the data;

(b) limit the use of the FIS to the detection, investigation or prosecution of offences that carry a maximum penalty of not less than three years' imprisonment;[15]

(c) define 'identification information' and 'identity-matching service' or, alternatively, amend proposed paragraphs 5(1)(n) and 7(1)(f) to provide for a regulation-making power;

(d) require the Minister to report to the public on the results of the consultations with the Australian Human Rights Commissioner and the Australian Information Commissioner before any rules are made to prescribe additional types of identification information or new identity-matching services, or any other rules or regulations relating to identity-matching services, and require the Minister to provide reasons explaining why rules depart from that advice if they do;

(e) ensure that identification information produced in response to a request for an identity-matching service is not used for any purpose other than establishing or verifying the identity;

(f) make it clear whether 'identification information' is 'sensitive' 'personal information' for the purposes of the *Privacy Act 1988* (Cth) and if 'identification information' is not 'sensitive' 'personal information', such a departure from existing privacy standards be expressly articulated to allow for a full and informed debate;

(g) require users of the identity-matching services to have appropriate facial recognition training in addition to special training to ensure that in the performance of duties they respect as well as protect human rights of all persons without distinction as to race, colour or ethnic origin;[16]

(h) require that an annual report on the interoperability hub includes:

(i) details of the non-government entities that access the FVS;

---

[15] The Law Council recognises that this requirement is provided for in the Face Identification Service (FIS) Access Policy: Department of Home Affairs, Face Identification Service (FIS) Access Policy - National Facial Biometric Matching Capability (Version 2.4, August 2018) cl 4.1(b) <https://www.homeaffairs.gov.au/criminal-justice/files/face-identification-service-fis-access-policy.pdf>. However, provision is also made for the use of the FIS for 'queries for the permitted purpose of community safety', which 'recognises that there may be circumstances which warrant the use of the FIS to help prevent harm to an individual or the broader community but **which do not involve a serious offence'**: cl 5.9 [emphasis added].

[16] The Law Council recognises that some training for Nominated Users is mandated in the FIS and FVS Access Policies: Department of Home Affairs, FIS) Access cls 6.20-6.22; Department of Home Affairs, FVS Access Policy cls 3.18-3.19.

(ii) the number of false matches generated by the identity-matching services that incorrectly identify an individual;

(iii) data breaches and system outages;

(iv) the number of instances in which an entrusted person discloses protected information to lessen or prevent a threat to life or health;

(v) Australian Security Intelligence Organisation's use of the interoperability hub, determined on a case by case basis;[17]

(i) establish a new regulatory authority with responsibility for the oversight of the retention, collection and use of biometric information;

(j) establish a new advisory and oversight board of the identity-matching services proposed by the IMS Bill, potential membership including the Australian Information and Privacy Commissioner, a new Biometrics Commissioner, the Ministerial Council for Police and Emergency Management and the Australian Human Rights Commissioner;

(k) require the Office of the Australian Information Commissioner (**OAIC**) to undertake annual privacy assessments in relation to the interoperability hub contained in the IMS Bill, rather than in the Memorandum of Understanding between the Department and participating agencies;

(l) have an independent body undertake the Department's review responsibilities, such as the review of the agreements between the Department and participating agencies and the review of the audits and compliance reports submitted by participating agencies;

(m) ensure independent and effective scrutiny is in place to specifically assess the adequacy of measures to protect individuals against being discriminatorily targeted and profiled; and

(n) require that the agreements between participating agencies and the Department, and the interagency agreements be publicly available**.**

18. These recommendations are discussed in further detail below.

Proposed face-matching services in Australia

19. The identity-matching services that will be established and facilitated by the Department will 'make available tools to enable agencies to more securely share and match information'[18] with a view to allowing for the rapid identification of people.[19]

20. The Law Council reiterates the view expressed in its previous submission that the identity matching services operating through the interoperability hub may have the

[17] The Law Council recognises that annual reports are published by the Controller Hub, however the Law Council considers that these provisions should be contained in primary legislation rather than departmental policy: Department of Home Affairs, FIS Access Policy, cl 6.29; Department of Home Affairs, FVS Access Policy, cl 3.27.
[18] Department of Home Affairs, Submission No 12.1 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018* (May 2018) 15 [82]. <https://www.aph.gov.au/DocumentStore.ashx?id=ee184fa7-8b1f-4f65-a0e2-a7129d782fe4&subId=564903>.
[19] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) 52.

effect of undermining informed consent by individuals in relation to their personal information.[20] Many government services are required to participate fully in society and are therefore essential in practice for individuals.[21] In the case of the FVS, a person who requires an important service, such as the provision of a driver licence, may not have a genuine choice to decline to have their identity verified through a face-matching service. Further, a person may have consented to providing a photograph to obtain a driver licence but have not consented to their biometric information being extracted from that image and being used for other purposes.[22] It must be ensured that the use of images beyond those consented to is not permissible.

21. In addition, the increase in the speed in which an individual may be identified on a one-to-many image-based biometrics matching from a facial image captured from CCTV footage is likely to lead to an increase in the number of requests that will pass through the interoperability hub, which is the objective of the proposed legislation.[23] An increased capability for more rapid, targeted searching using still facial images from CCTV to promptly identify a person of interest for public safety purposes necessitates appropriate, independent oversight given the potential encroachment of individuals' privacy.

22. Therefore, the Law Council considers that it is critical that the concerns expressed about the IMS Bill, particularly ensuring robust privacy protections and oversight measures, are addressed before being passed by Parliament.

An increase in facial recognition technology integrated with CCTV

23. The Law Council understands that in the evidence provided by the Department to the Committee at its hearing on 17 August 2018, it was stated that the framework for the automated sharing of biometric data between federal, state and territory government agencies, and in some cases local government and private sector organisations, is not intended for mass surveillance and would not include live video feeds.[24] The Department stated that the system could not be hooked up to a live feed to provide real-time facial recognition of people in a public place.[25]

24. In the Northern Territory, Queensland and Western Australia, facial recognition technology which has been integrated with CCTV systems has been trialled.[26]

25. In Queensland, the *Police and Other Legislation (Identity and Biometric Capability) Amendment Act 2018* (Cth) (**Identity and Biometric Capability Act**) was enacted in March 2018, amending a range of transport and policing laws to authorise

---

[20] Law Council of Australia, Submission No 8 to the Parliamentary Joint Committee on Intelligence and Security, *Review into the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018* (21 March 2018) 3 [12].
[21] See Evidence to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 3 May 2018, 16 (Mr Peter Leonard, Law Council of Australia).
[22] Law Council of Australia, Submission No 8 to the Parliamentary Joint Committee on Intelligence and Security, *Review into the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018* (21 March 2018) 3 [12].
[23] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) 3 [12].
[24] Rohan Pearce, 'Biometrics: Govt Plays Down Concerns Over Mass Surveillance' *Computer World* (Web Page, 17 August 2018) <https://www.computerworld.com.au/article/645384/biometrics-govt-plays-down-concerns-over-mass-surveillance-private-sector-access/>; Joseph Brookes, 'Australia's Dangerous Foray into Facial Recognition', *Which-50* (Web Page, 5 August 2019) <https://which-50.com/cover-story-australias-dangerous-foray-into-facial-recognition/>.
[25] Ibid.
[26] Department of Parliamentary Services (Cth), *Bills Digest* (Digest No 21 of 2019-20, 26 August 2019) 7.

Queensland's participation in the identity-matching scheme under Intergovernmental Agreement.[27]

26. The Queensland Government stated that the Identity and Biometric Capability Act was passed to 'significantly benefit the security operation for the [Commonwealth] Games'[28] as it would 'allow the comparison of images with immigration and citizenship records held by Australian Government agencies and enable the rapid identification of people'.[29] At the time, the Queensland Government 'envisaged that other agencies will come on board to share their holdings' and encouraged 'the Federal Government and all states and territories to ensure this legislation is passed in time for the Commonwealth Games'.[30]

27. In May 2019, the Queensland Police Service's evaluation report of the facial recognition system used during the Commonwealth Games was obtained by ABC News under the *Right to Information Act 2009* (Qld). This evaluation reported problems with the system's rollout:

> *Difficulties were experience in data ingestion into one of the systems with the testing and availability not available until the week Operation Sentinel [the Games security operation] commenced…*
>
> *The inability of not having the legislation passed, both Commonwealth and state, in time for the Commonwealth Games reduced the database from an anticipated 46 million images to approximately eight million.*[31]

28. There were 16 high-priority targets requested as part of Operation Sentinel, however none could be identified. It was reported that police records were included but images from Queensland's Department of Transport and Main Roads were not. Halfway through the duration of the Commonwealth Games, the system was 'opened up to basic policing', which provided only five identities out of the 268 requested.[32]

29. Trials of a similar technology are currently taking place in Perth, where a twelve-month trial using facial recognition technology in 30 CCTV cameras installed across East Perth is underway.[33] It is reported that the technology scans and stores the biometric data of individuals, which is then allegedly matched against photos, such as those stored in the Australian Government's biometric database.[34] In June 2019, there were reports that Stadiums Queensland has 'admitted to trialling facial recognition software on sports fans and concertgoers'.[35] Furthermore, in the Northern Territory, Darwin

---

[27] *Intergovernmental Agreement of Identity Matching Service* (5 October 2017) <https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf>.
[28] Mark Ryan, Minister for Police and Minister for Corrective Services Queensland. 'Queensland Leads Nation to Strengthen Security Measures' (Media Statement, 7 March 2018) <http://statements.qld.gov.au/Statement/2018/3/7/queensland-leads-nation-to-strengthen-security-measures>.
[29] Ibid.
[30] Ibid.
[31] Josh Bavas, 'Facial Recognition System Rollout Was Too Rushed, Queensland Police Report Reveals', *ABC News* (online, 6 May 2019) <https://www.abc.net.au/news/2019-05-06/australias-biggest-facial-recognition-roll-out-rushed/11077350>.
[32] Ibid.
[33] Rebecca Turner, 'City of Perth Rolls Out New Facial Recognition CCTV Cameras, But Is It Surveillance By Stealth?', *ABC News* (online, 8 June 2019) <https://www.abc.net.au/news/2019-06-08/city-of-perth-rolls-out-new-facial-recognition-cctv-cameras/11147780>.
[34] Ibid.
[35] Josh Bavas, 'Facial Recognition Quietly Switched on at Queensland Stadiums, Sparking Privacy Concerns', *ABC News* (online, 6 June 2019) <https://www.abc.net.au/news/2019-06-05/facial-recognition-quietly-switched-on-at-queensland-stadiums/11178334>.

Council is adopting 138 new CCTV cameras which have inactive facial recognition technology capabilities.[36]

30. The Law Council further notes that in its submission on the 2018 Bills, the Department had envisaged that the FIS would be used to match images from CCTV, for example, in the following ways:

    (a) a specialist counter-terrorism team could use the Advance Identify Subject Request function of the FIS to submit facial images from CCTV to seek a match against several government identity holdings (passports, visas and drivers' licences) to determine the suspect's identity;[37] and

    (b) law enforcement could submit a still image taken from CCTV to identify a suspected paedophile from child exploitation material, or to identify an armed robber.[38]

31. The Department noted that:

> *[the FIS] will not be used for minor offences such as littering or parking infringements, but it may be used to help identify victims of disasters and to locate missing persons*.
>
> *Access to the FIS will only be provided to a limited number of users in specialist areas with training in how to interpret the results. It does not provide for fully automated or 'real time' surveillance of public spaces, but does enable more targeting searching using still images, taken from CCTV for example, to quickly identify a 'person of interest' for public safety purposes*.[39]

32. The Law Council recognises that the IMS Bill:

> *…simply enable[s] the Department to make available tools to enable agencies to more securely share and match information. The key principle on which the services operate is that all participating agencies must have their own legal basis to collect, use and disclose the information they share through the services. This also applies to their collection of the primary biometric information from an individual (such as the collection of CCTV footage or passport photos), and their retention of that information for use through the services or otherwise. [The IMS Bill] does not seek to expand police powers in relation to collection or retention of biometrics, nor authorise agencies other than the Department to use or share information where it is not otherwise authorised under other legislation*.[40]

---

[36] Chris Griffith, 'Surveillance Cameras with AI are Watching You', *The Australian* (online, 29 August 2019) <http://online.isentialink.com/theaustralian.com.au/2019/08/28/5a0c1e07-c84d-49e3-b516-2151ebd8f0ef.html>; Lauren Roberts, 'Darwin Council's Original Plan was to Use Facial Recognition', *NT News* (online, 19 August 2019) <https://www.ntnews.com.au/news/darwin-councils-original-plan-was-to-use-facial-recognition/news-story/c219622392ed6e6d241ecf64a25022a3>

[37] Department of Home Affairs, Submission No 12.2 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018* (May 2018) 9 <https://www.aph.gov.au/DocumentStore.ashx?id=0e002969-34c5-45db-8b51-505f1026b8ce&subId=564903>.

[38] Ibid 11.

[39] Ibid.

[40] Department of Home Affairs, Submission No 12.1, 25 [82].

Independent oversight and governance

Threshold for offences

33. An increased capability for more targeted searching using still facial images from CCTV to promptly identify a person of interest for public safety purposes necessitates appropriate, independent oversight given the potential encroachment of individuals' privacy. The Department acknowledges impacts on individuals' privacy, as it recognises that, in some instances, it is less clear that the public benefit in using the FIS outweighs the potential privacy impacts on individuals.[41] For example, the Department considers that the broader public interest of using the FIS to prevent harm to individuals or the broader community, but which does not involve 'serious offences', does not clearly outweigh the potential privacy impacts on individuals.[42]

34. While the Department states that the FIS will not be used for 'minor offences such as littering or parking infringements',[43] the FIS could potentially be used for the prevention, detection, investigation and prosecution of minor offences which arguably cause harm to an individual or the broader community but do not carry a maximum penalty of no less than three years' imprisonment.

35. The Law Council notes that the Intergovernmental Agreement states that the FIS can only be used for one or more of the 'permitted purposes'.[44] In respect of the detection, investigation or prosecution of an offence, it states that this should be an offence carrying a maximum penalty of not less than three years' imprisonment. However, that element is not present in the IMS Bill.[45]

36. The Law Council notes that the Senate Standing Committee for the Scrutiny of Bills has expressed concern that the IMS Bill may unduly trespass on personal rights and liberties in seeking to enable the sharing 'of an extensive amount of personal information for a broad range of purposes to a broad range of agencies'.[46] Part of the reason for this concern arises because, as currently drafted, the IMS Bill will allow state and territory agencies to share and seek to match facial images and other biographical information for persons suspected of involvement in minor offences.

37. The Law Council considers that this may not be a necessary or proportionate response and that aspect of the IMS Bill may constitute an arbitrary interference with the right to privacy in conflict with Article 17 of the ICCPR.[47]

38. The Law Council considers that the use of the FIS should be reserved for the prevention, detection, investigation and prosecution of serious offences. To this end, the IMS Bill should include a provision which limits the use of the FIS to the detection, investigation or prosecution of offences that carry a maximum penalty of not less than three years' imprisonment.[48]

---

[41] Department of Home Affairs, FIS Access Policy, cl 5.6
[42] Ibid.
[43] Department of Home Affairs, Parliament of Australia, 'Face Matching Services' (Fact Sheet) 1 <https://www.homeaffairs.gov.au/criminal-justice/files/face-matching-services-fact-sheet.pdf>.
[44] *Intergovernmental Agreement of Identity Matching Service* (5 October 2017) [4.21].
[45] See Evidence to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 3 May 2018, 17 (Mr Peter Leonard, Law Council of Australia).
[46] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Scrutiny Digest 2 of 2018, 14 February 2018) 22-23.
[47] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 993 UNTS (entered into force 3 January 1976) art 17.
[48] The Law Council recognises that this requirement is provided for in the Face Identification Service (FIS)

39. If the IMS Bill is not amended to include a provision that implements the three-year 'offence threshold', it is even more essential for robust, independent oversight measures to be present.

Independent oversight

40. Given the potential broad use of the FIS and impacts on individual privacy, the Law Council considers that it would be more appropriate for an independent body or authority to audit the Department's identity-matching service agreements and systems, rather than the Department itself.

41. The FIS Access Policy and FVS Access Policy provide that a 'Requesting Agency'[49] must engage an independent auditor to audit all of its data sharing via the FIS at least once every financial year.[50]

42. The Law Council recognises that the OAIC has entered into a Memorandum of Understanding with the Department for annual audits for 2017-18 and 2018-19.[51] However, this is limited to conducting a privacy assessment.[52] The Law Council notes that the audits undertaken by the Requesting Agencies, along with compliance reports, are reviewed by the Department, with no external oversight.[53]

43. The Law Council reiterates its recommendation that the requirement for OAIC to undertake annual privacy assessments in relation to the interoperability hub be contained in the IMS Bill, rather than in the Memorandum of Understanding between the Department and participating agencies. While it is the view of the Department the IMS Bill is 'not intended to govern the full operation and use of the identity-matching services',[54] the Law Council considers that the OAIC's oversight role should be ensured into the future by including a provision to such effect in the primary legislation.

44. Furthermore, the Law Council notes that the *Privacy (Australian Government Agencies — Governance) APP Code 2017*, as updated on 25 July 2019, requires that there be an express requirement to undertake a Privacy Impact Assessment as this is a 'high privacy risk' project.[55]

Access Policy: FIS Access Policy cl 4.1(b). However, provision is also made for the use of the FIS for 'queries for the permitted purpose of community safety', which 'recognises that there may be circumstances which warrant the use of the FIS to help prevent harm to an individual or the broader community but *which do not involve a serious offence'*: cl 5.9 [emphasis added].

[49] See Memorandum of Understanding, 7 definition of 'requesting agency'.

[50] This must include, inter alia, an examination of the queries relating to the permitted purpose of community safety, considering the greater privacy risk and whether authorisation was obtained for those circumstances that required authorisation: Department of Home Affairs, FIS Access Policy, cl 6.24.

[51] For the years 2017/8 and 2018/9, the Attorney-General's Department signed a Memorandum of Understanding with the Office of the Australian Information Commission (OAIC) to conduct a privacy assessment of the National Facial Biometric Matching Capability. On the OAIC's website, any agreement between the Department and OAIC could not be found: Office of the Australian Information Commissioner, 'MOU with AGD — National Facial Biometric Matching Capability' (Web Page, 21 May 2019) <https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-of-understanding/mous/mou-with-agd-national-facial-biometric-matching-capability/>.

[52] The template of the Memorandum of Understanding between the Department and agencies states that the Department commits to conducting a privacy assessment in relation to the National Facial Biometric Matching Capability 'by an independent entity': *National Facial Biometric Matching Capability, Face Matching Services – Services*, *The Department of Home Affairs and the Agency* (Template Memorandum of Understanding) 13 [14.7].

[53] Department of Home Affairs, FIS Access Policy, cl 10.1.

[54] Department of Home Affairs, Submission 12.1, [58].

[55] Office of the Australian Information Commissioner, *Privacy (Australian Government Agencies – Governance) APP Code 2019* (26 October 2017) cl 12(1).

45. The Law Council further recommends that the Department's review responsibilities, such as the review of the agreements between the Department and participating agencies and the review of the audits and compliance reports submitted by participating agencies, be conducted by an independent body.

46. To that end, the Law Council again recommends that the Committee fully consider the utility of establishing a new regulatory authority with responsibility for this role. This would allow oversight to be conducted thoroughly and by an agency with a sole focus on, and expertise in, biometric data. The Law Council notes again the UK's Commissioner for the Retention and Use of Biometric Material (**UK Biometrics Commissioner**), which was established to ensure that there is an office responsible for governing the retention and use of biometric information in the UK.

47. The Law Council recognises the Department's view that the role of the UK Biometrics Commissioner primarily relates to the review of the retention and use by the police of DNA samples, profiles and fingerprints, and police use of facial biometrics. The Department considers that as the IMS Bill will 'facilitate information-sharing between agencies that already have a legal basis to do so', the oversight of existing or new police powers in relation to biometric information falls outside the scope of the IMS Bill.[56]

48. In response to the Department's position, the Law Council notes that the UK Home Office has recognised the need for greater oversight of biometrics technology and has taken action to this end. In response to a recommendation from the House of Commons Select Committee on Science and Technology (**House of Commons Committee**), the Home Office established the Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board (**Oversight and Advisory Board**).[57] The Oversight and Advisory Board's purpose is to look at the development and use by police forces of:

    (a) facial image storing and matching systems;

    (b) new biometrics other than DNA, fingerprints and facial images - this includes voice, iris, finger vein and gait recognition; and

    (c) sharing of facial images collected by police forces with other agencies.[58]

49. The Oversight and Advisory Board brings together representatives from the list below to allow open dialogue between those considering using facial recognition and new biometric technology:[59]

    (a) police;

    (b) Association of Police and Crime Commissioners;

    (c) Home Office;

---

[56] Ibid [41]-[42].
[57] Select Committee on Science and Technology, *Biometrics Strategy and Forensic Services* (House of Commons, 5th Report, Session 2017-19, 23 May 2018) 23 [55] <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf>.
[58] United Kingdom Government, 'Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board' (Web Page) <https://www.gov.uk/government/groups/law-enforcement-facial-images-and-new-biometrics-oversight-and-advisory-board>.
[59] Ibid.

(d) Surveillance Camera Commissioner;[60]

(e) Biometrics Commissioner;

(f) Information Commissioner's Office;[61]

(g) Forensic Science Regulator; and

(h) Biometrics and Forensic Ethics Group.

50. The Home Office's establishment of this oversight body demonstrates the need for robust oversight of not only the powers of law enforcement to collect biometric information, but also of matching systems and information sharing between agencies. The Law Council recommends that a board of a similar nature should be established in Australia, with potential membership including the Australian Information and Privacy Commissioner, a new Biometrics Commissioner, the Ministerial Council for Police and Emergency Management and the Australian Human Rights Commissioner.[62]

Transparency measures

51. Identity-matching services are legitimised through citizen trust of what governments are doing. The Explanatory Memorandum states:

> *Accountability and transparency are also essential in data-sharing between government agencies. Members of the community have a right to understand how governments are sing their identification information, and to have access to publicly available information about those uses. This is an essential aspect of a free and democratic society that supports trust in government processes and services*.[63]

52. To this end, the Law Council recommends that the agreements between participating agencies and the Department, and the interagency agreements be publicly available.

53. In addition, the Law Council reiterates the point made in its previous submission that there remain flaws with existing facial recognition technologies.[64] Issues relating to reliability and accuracy of facial recognition technologies have been recognised in the UK context (see below paragraphs 61, 62 and 71), as well as by the Department.[65]

---

[60] The Surveillance Camera Commissioner is the statutory regulator of surveillance cameras whose specific powers and responsibilities are set out in section 34 of the *Protection of Freedoms Act 2012* (UK) with regard to encouraging compliance with the Surveillance Camera Code of Practice. Responsibilities include, in particular, regulating the use of surveillance cameras and their use on conjunction with automated facial recognition technology: *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341, [9].

[61] The Information Commissioner has specific statutory powers and responsibilities under Part 5 of the *Data Protection Act 2018* (UK).

[62] The membership of the Ministerial Council for Police and Emergency Management is Ministers for Police and Emergency Management from the Commonwealth, each State and Territory, New Zealand, and the President of the Australian Local Government Association: Department of Home Affairs, 'Ministerial Council for Police and Emergency Management' (Web Page) <https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/committees-and-fora/ministerial-council-police-emergency-management>.

[63] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) 55.

[64] Law Council of Australia, Submission No 8 to the Parliamentary Joint Committee on Intelligence and Security, *Review into the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching services) Bill 2018* (21 March 2018) 4, [16].

[65] Department of Home Affairs, Submission 12.1, [118].

54. The Law Council recognises the existing measures which seek to minimise the risk of false matches. For the FVS, its functionality is limited to 'one-to-one' matching and a 'match or no-match response'. For the FIS, the one-to-many matching will not rely on a completely automated process to identify a person. In both cases, a match should not be relied upon by a user as the sole basis for making an identity resolution decision.[66]

55. Nonetheless, the Law Council maintains the view that additional technical information about the nature of the identity matching services and the process for ensuring that there are not false matches should be released publicly to allow informed debate about the proposed legislation. The annual report on the interoperability hub should include the number of false matches generated by the identity-matching services that incorrectly identify an individual.

Potential for future scope expansion

56. The Law Council is concerned that the IMS Bill as currently drafted would not provide for adequate scrutiny in the event that the list of 'identification information' in proposed subsection 5(1) were to be expanded. This is due to the power contained in proposed paragraph 5(1)(n) that 'identification information' includes 'any information prescribed by the rules and relates to the individual'.

57. The Law Council notes that a similar power exists for the addition of new identity-matching services, as proposed paragraph 7(1)(f) provides that rules can prescribe that a service is an 'identity matching service'.

58. The source of the Law Council's concern is that the data sources used by the identity-matching services could grow past the currently intended sources, such as passports, visas and road licences,[67] to a much larger, more intrusive set of data sources, such as charge photos and prison photos, without a sufficient level of parliamentary scrutiny and oversight. Furthermore, entirely new services for the collection, use and disclosure of identification information that involve the use of the interoperability hub could be introduced without the parliamentary scrutiny to which primary legislation is subjected.

59. The Law Council recognises that proposed section 30 of the IMS Bill states that rules made under proposed paragraphs 5(1)(n) and 7(1)(f) will be legislative instruments for the purposes of the *Legislation Act 2003* (Cth)[68] and that rule made under those paragraphs would be subject to disallowance and sunsetting.[69]

60. While this provides a degree of parliamentary scrutiny of the rules that could be made to expand the list of 'identification information' or 'identity-matching services', the Law Council considers that greater scrutiny is required. This could be achieved if proposed paragraphs 5(1)(n) and 7(1)(f) provided a power to make regulations rather than rules.

61. The Law Council acknowledges the Department's rationale for including a rule-making power for the expansion of 'identification information' and 'identity-matching services'.

---

[66] Ibid [112].
[67] Identity-Matching Services Bill 2019 (Cth) cls 5(1)(g)-(m). See Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) 14 [62].
[68] Under sections 38 and 39 of the *Legislation Act 2003* (Cth), legislative instruments and their explanatory statements must be tabled in Parliament and within six days of registration of the instrument on the Federal Register of Legislation. The rules would be able to be scrutinised by the Senate Standing Committee on Regulations and Ordinances.
[69] Identity-Matching Services Bill 2019 (Cth) cls 30(3)-(4).

It contends that the approach currently provided in the IMS Bill is appropriate because it is consistent with the Office of Parliamentary Counsel's *Drafting Direction No 3.8*, which provides that 'subordinate instrument should be made in the form of legislative instruments as distinct from regulation unless there is a good reason to do so'.[70] In its view, the advantages that would come from the use of rules rather than regulation, such as allowing for the use of a single type of legislative instrument and for the simplification of language and structure in the IMS Bill,[71] render it appropriate to include a rule-making power, rather than regulation-making power, in proposed paragraphs 5(1)(n) and 7(1)(f).

62. The primary position of the Law Council is that 'identification information' and 'identity-matching services' should only be defined in the primary legislation. This is key to addressing function creep and ensuring accountability.

63. If a power to expand these definitions by subordinate legislation remains in the IMS Bill, the position of the Law Council is that this should be a regulation-making power. The Law Council submits that there is a good reason to include a regulation-making power, that being that proposed paragraphs 5(1)(n) and 7(1)(f) of the IMS Bill largely define the boundaries of the identity-matching services: they determine what and how information about an individual can be collected and shared for the purposes of obtaining or verifying a person's identity. For this reason, any expansions of this list should be subject to the higher level of scrutiny than is involved in the creation of regulations.

64. If a rule-making power or regulation-making power is used, the Law Council considers that the IMS Bill should go beyond the current requirement to consult with the Australian Human Rights Commissioner and Australian Information Commissioner. Prior to such rule or regulation being made, the Minister should be required to report to the public on the results on these consultations and provide reasons explaining why rules or regulations depart from that advice.

International experiences with facial recognition technology

Automated facial recognition technology: The United Kingdom

65. The use of 'live' or automated facial recognition technology in London and South Wales has been subject of much debate in the UK. The Law Council acknowledges that the types of identity-matching services that would be established by the IMS Bill are different to the automated facial recognition technology used in the UK, which involves data-processing algorithms automatically mapping the biometric details of individuals and undertaking a comparison to those stored on a database.[72] Nonetheless, the issues in the UK arising from the broad surveillance of the population through facial recognition capabilities, provide a cautionary tale for Australia.

66. Furthermore, it is important to recognise that the legal safeguards present in the UK which are not replicated in Australia. This includes the protection of human rights, including the right to privacy, in the *Human Rights Act 1988* (UK) (**Human Rights**

[70] Office of Parliamentary Counsel, *Drafting Direction No. 3.8: Subordinate Legislation* (July 2017) [2].
[71] Department of Home Affairs, Submission 12.1 [129]-[133].
[72] *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341, [25].

Act)[73] and the legal protections and safeguards afforded to the individuals' data, including biometric data, under the *Data Protection Act 2018* (UK) (**Data Protection Act**).[74] Additionally, there are stronger oversight and governance measures relating to biometric data collection and use in the UK, including the existence of the Biometrics Commissioner, the Surveillance Camera Commissioner, the Oversight and Advisory Board and the Ethics Group.

67. While it was recently determined by the High Court of Justice of England and Wales that South Wales Police's deployments of automated facial recognition was lawful (discussed below) this case provides an example of how these legal frameworks can used as a check and balance on the use of facial recognition technology in the UK.[75] The High Court of Justice of England and Wales held that the use of the automated facial recognition technology did not breach the first data protection principle in Data Protection Act, which ensures that the processing of personal data for law enforcement purposes is lawful and fair, and that this use of automated facial recognition technology was in accordance with the law' for the purposes of the Human Rights Act.[76] The absence of similar rights frameworks in Australia renders it critical that the IMS Bill legislates boundaries for reasonable and proportionate use of identity-matching services and robust safeguards and oversight measures.[77]

68. In the UK, automated facial recognition technology has been integrated with CCTV systems to enable police to identify persons suspected of committing an offence and subjects of an arrest warrant.[78] Between 2016 and 2019 the London Metropolitan Police Service (**LMPS**) conducted 10 test deployments, trialling automated facial recognition technology during policing operations. The Neoface system used by the LMPS was also used by police in South Wales.[79] . The use of automated facial recognition technology by the police and private companies has been troubled. A private company's use of automated facial recognition technology on the public in the King's Cross area of London[80] sparked the Information Commissioner to launch an investigation into how the technology is used and an inspection of the system and its operation in order to assess whether it complies with the Data Protection Act.[81]

69. In May 2018, the House of Commons Select Committee on Science and Technology (**House of Commons Committee**) recommended that*:*

> *Facial image recognition provides a powerful evolving technology which could significantly help policing. There are serious concerns, however, over its current use, including its reliability and its potential for discriminatory bias. We welcome the Government's assurances that the technology is only being used at the*

---

[73] The *Human Rights Act 1988* (UK) domestically implements the *Convention for the Protection of Human Eights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).
[74] *Data Protection Act 2018* (UK) pt 3.
[75] *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341.
[76] Ibid [96]; *Convention for the Protection of Human Eights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) art 8.
[77] *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341 [133]; *Data Protection Act 2018* (UK) s 35.
[78] Department of Parliamentary Services (Cth), *Bills Digest* (Digest No 21 of 2019-20, 26 August 2019) 7.
[79] Pete Fussey and Daragh Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology (Human Rights Centre, University of Essex, July 2019).
[80] Elizabeth Denham, Information Commissioner, 'Live Facial Recognition Technology in King's Cross' (Statement, 15 August 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/>.
[81] Ibid.

moment for targeting those on 'watch lists' rather than as a blanket approach, and that images collected from public events and the relevant watch lists are being deleted afterwards.

Facial recognition technology should not be generally deployed, beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved. The new facial images 'oversight Board' that the Minister is planning to set up will need to ensure that that condition is satisfied. But in such an important area, with public confidence critical, it must be ministers and Parliament that take the final decision on any wider deployment of the technology. The forthcoming Biometrics Strategy should include an undertaking that such a decision will not be left to be "an operational decision for the police", and provide a Government commitment to give the House an opportunity to debate and vote on the issue.[82]

70. In February 2019, the Biometrics and Forensics Ethics Group Facial Recognition Working Group (**UK Working Group**) released its interim report on the ethical issues raised by the use of automated facial recognition technology for policing purposes.[83] The UK Working Group recognised the ongoing concerns about the accuracy of the technology, its potential for biased outputs and an ambiguity in the nature of the then current deployments. The UK Working Group noted the lack of independent oversight and governance and drafted a number of ethical principles that can be used to inform any future deployments.[84]

71. In March 2019, the House of Commons Committee held a one-off hearing on biometrics and forensics to follow up on the Committee's recommendations from its 2018 Report on Forensic Science.[85]

72. As part of this inquiry, the Information Commissioner expressed to the House of Commons Committee that such a deep concern was held about the use of automated facial recognition technology by police in some areas that a priority investigation was opened to understand and investigate the use of automated facial recognition by law enforcement in public spaces.[86] This investigation will be completed later in 2019 and will include the consideration of 'the legal basis, the necessity, proportionality and justification for this intrusive processing'.[87] The Information Commissioner was particularly concerned about the ambiguity of the trials, as well as the broader use of automated facial recognition and whether the trials demonstrate full compliance with the Data Protection Act.

73. The Biometrics Commissioner also told the House of Commons Committee that the trials should be conducted in a more consistent, standardised and robust way, which

---

[82] Select Committee on Science and Technology, *Biometrics Strategy and Forensic Services* (House of Commons, 5th Report, Session 2017-19, 23 May 2018) 21 [49], [50] <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf>.
[83] Biometrics and Forensics Ethics Group Facial Recognition Working Group, *Ethical Issues Arising from the Police Use of Live Facial Recognition Technology* (Interim Report, February 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf>.
[84] Ibid Annexes A, B.
[85] Select Committee on Science and Technology, *The Work of the Biometrics Commissioner and the Forensic Science Regulation* (House of Commons, 19th Report, Session 2017-19, 7 July 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf>.
[86] Steve Wood, Information Commissioner's Office, Submission to the Select Committee on Science and Technology, *The Work of the Biometrics Commissioner and the Forensic Science Regulation* (March 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf>.
[87] Ibid.

would allow for proper academic review while avoiding function creep from a trial to an extended deployment.[88]

74. The House of Commons Committee reiterated its recommendation from its 2018 Report that automatic facial recognition should not be deployed until concerns over the technology's effectiveness and potential bias have been fully resolved. It called on the Government to issue a moratorium on the current use of facial recognition technology and no further trials should take place until a legislative framework has been introduced and guidance on trial protocols, and an oversight and evaluation system, has been established.[89]

75. The House of Commons Committee also criticised the UK Government's 'Biometrics Strategy', released in June 2018, for:

    (a) lacking 'a coherent, forward looking vision';

    (b) failing 'to address the legislative vacuum that the Home Office has allowed to emerge around new biometrics';

    (c) missing the opportunity to set out a principles-based approach to the use and oversight of second-generation biometrics;

    (d) establishing an oversight board with no legal powers given the highly intrusive nature of the technologies; and

    (e) having poor engagement with the public in the development of the strategy.[90]

76. Civil society groups have further criticised the automated facial recognition trials. Professor Peter Fussey and Dr Daragh Murray at the University of Essex's Human Rights Centre (**Human Rights Centre**) undertook an independent academic report on the trials by LMPS by observing the final six test deployments in Soho, Romford and at the Westfield shopping centre in Stratford from June 2018.[91] The Human Rights Centre published its report in July 2019, which highlighted a number of issues arising from the automated facial recognition test deployments.

77. The key concerns of the Human Rights Centre was the absence of an explicit legal basis for the use of automated facial recognition, the inadequacy of the implicit legal basis identified by the LMPS in relation to the 'in accordance with the law' requirement established by human rights law, and that the LMPS' test deployments of automated facial recognition would not be regarded as 'necessary in a democratic society' if challenged before the courts.[92]

78. Further concerns were had regarding the research process adopted by the LMPS to trial automated facial recognition technology and operational factors relating to inconsistency in the adjudication process, including a presumption to intervene, as well as difficulties with how the LMPS engaged with individuals and in obtaining the consent of those affected.[93]

---

[88] Select Committee on Science and Technology, *The Work of the Biometrics Commissioner and the Forensic Science Regulation* (House of Commons, 19th Report, Session 2017-19, 7 July 2019) 15 [32] <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf>.
[89] Ibid 16 [37].
[90] Ibid 13 [27].
[91] Pete Fussey and Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (Human Rights Centre, University of Essex, July 2019).
[92] Ibid 8-10.
[93] Ibid 10-3.

79. Regarding operational and reliability issues, the organisation Big Brother Watch uncovered the following using a series of Freedom of Information requests:

    (a) South Wales Police store photos of all innocent people incorrectly matched by facial recognition for a year, without their knowledge, resulting in a biometric database of over 2,400 innocent people;

    (b) LMPS' facial recognition matches were 98 per cent inaccurate, misidentifying 95 people at last year's Notting Hill Carnival as criminals – yet carried out 7 more deployments in 2018; and

    (c) South Wales Police's matches were 91 per cent inaccurate – yet continued to target concerts, sports matches and Christmas markets in 2018.[94]

80. In March 2019, the LMPS paused its use of facial recognition and is currently deciding whether to continue use of the technology. In May 2019, it was reported that the LMPS had not yet made a decision on its future use of automated facial recognition.[95]

81. In September 2019, the High Court of Justice of England and Wales was one of the first courts in the world to consider automated facial recognition.[96] A claimant whose face was scanned by an automated facial recognition camera while in public bought a case against South Wales Police's use of the technology on the grounds that such use was contrary to the requirements of the Human Rights Act, the Data Protection Act and that the decision to implement or use it had not been taken in accordance with the public sector equality duty contained in the *Equality Act 2010* (UK).

82. The High Court of Justice of England and Wales held that the use of automated facial recognition was 'in accordance with the law' for the purposes of the Human Rights Act.[97] It was held that while the technology infringed on the right to privacy,[98] there existed a framework for the legal underpinning of the use of automated facial recognition,[99] which ensured that the interference with the right to privacy was in accordance with law.[100]

83. In addition, the High Court of Justice of England and Wales held that the use of the automated facial recognition technology did not breach the first data protection principle in Data Protection Act, which ensures that the processing of personal data for law enforcement purposes is lawful and fair.[101] On this principle, biometric data is afforded an additional level of protection,[102] which requires law enforcement agencies to rely on consent,[103] or to demonstrate that the processing is strictly necessary for a law enforcement purpose and is necessary for exercise of the police's functions and, at the time of processing, the South Wales Police had an appropriate policy in

---

[94] Big Brother Watch, 'Face Off' (Web Page, May 2019) <https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/#legalchallenge.
[95] Big Brother Watch, 'Stop the Met Police Using Authoritarian Facial Recognition Cameras', Crowd Justice (Web Page, 6 September 2019) <https://www.crowdjustice.com/case/face-off/>.
[96] *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341.
[97] Ibid [96].
[98] *Convention for the Protection of Human Eights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) art 8.
[99] *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341, [63]-[97].
[100] Ibid [98]-[103].
[101] *Data Protection Act 2018* (UK) s 35; *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341 [133].
[102] *Data Protection Act 2018* (UK) s 35(3).
[103] Ibid s 35(4).

place.[104] In this instance, these requirements were met.[105] It was also found that the South Wales Police complied with the requirement to undertake a Data Protection Impact Assessment (**DPIA**).[106]

84. The South Wales Police's DPIA states that 'justification, proportionality, legality, auditability and accountability, necessity and ethical arguments remain at the heart of [the DPIA]'.[107] Under the requirement to note the general legal considerations relating to the engagement and delivery of automated facial recognition technology, the following were identified as the main legal considerations in the use of this technology:

    (a) the right to privacy under the *European Convention of Human Rights* and the Human Rights Act;

    (b) the first data protection principle in Data Protection Act;

    (c) the disclosure and audit requirements under the *Crime Procedure and Investigations Act 1996* (UK);

    (d) the requirements relating to police handing of data that is in their possession under the Home Office's *Code of Practice on the Management of Police Information*;

    (e) the directed surveillance provisions of the *Regulation of Investigatory Powers Act 2000* (Cth);

    (f) the twelve guiding principles within the *Surveillance Camera Code of Practice*;

    (g) the requirements under the *Freedom of Information Act 2000* (Cth); and

    (h) the public sector equality duty under the *Equality Act 2010* (Cth).[108]

85. The Law Council considers that these main legal considerations for automated facial recognition technology as identified in the South Wales Police's DPIA highlights the legislative framework in the UK which can act as a check and balance on the use of the technology.

86. Furthermore, as stated above, in the United Kingdom the existence of the *European Convention on Human Rights*, domestically implemented in the UK by the Human Rights Act, and the General Data Protection Regulation, implemented by the Data Protection Act, provide avenues of judicial challenge to the collection and use of biometric data through facial recognition capabilities. In the absence of equivalent legislation in Australia, the Australian Parliament may wish to ensure that legislation enabling facial recognition technology use is carefully drafted and considered so that it is aimed at a legitimate objective and is reasonable and proportionate.

---

[104] *Data Protection Act 2018* (UK) s 35; *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341, [133].
[105] *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341, [135]-[142].
[106] *Data Protection Act 2018* (UK) s 64; *R v The Chief Constable of South Wales Police and the Secretary of State for the Home Department* [2019] EWHC 2341, [142]-[148].
[107] South Wales Police Privacy Impact Assessment (Version 4, 12 February 2019) 5 <https://swplive.blob.core.windows.net/wordpress-uploads/2018/04/PIA-draft-V4-002.pdf>.
[108] Ibid 5-10.

Ethics, principles and governance of facial recognition technology: The European Commission

87. The need for principles to underpin and guide the development of AI, including biometric technologies, is well recognised and understood. The Law Council brings to the Committee's attention the European Commission's development of ethics guidelines for AI and their concerns and warnings about the use of facial recognition technology.

88. The Law Council notes that the European Commission established a High-Level Expert Group on AI (**EU Expert Group**) in June 2018. As part of its mandate, in April 2019 the EU Expert Group published *Ethics Guidelines for Trustworthy Artificial Intelligence* (**Guidelines**).[109] The Guidelines provide that:

> *The Trustworthy AI has three components, which should be met throughout the system's entire life cycle: (1) it should be lawful, complying with all applicable laws and regulations (2) it should be ethical, ensuring adherence to ethical principles and values and (3) it should be robust, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm. Each component in itself is necessary but not sufficient for the achievement of Trustworthy AI. Ideally, all three components work in harmony and overlap in their operation. If, in practice, tensions arise between these components, society should endeavour to align them*.

89. The Guidelines also provide examples of critical concerns raised by AI, one of which is identifying and tracking individuals with AI:

> *AI enables the ever more efficient identification of individual persons by both public and private entities. Noteworthy examples of a scalable AI identification technology are face recognition and other involuntary methods of identification using biometric data (i.e. lie detection, personality assessment through micro expressions, and automatic voice detection). Identification of individuals is sometimes the desirable outcome, aligned with ethical principles (for example in detecting fraud, money laundering, or terrorist financing). However,* ***automatic identification raises strong concerns of both a legal and ethical nature, as it may have an unexpected impact on many psychological and sociocultural levels****. A proportionate use of control techniques in AI is needed to uphold the autonomy of European citizens.* ***Clearly defining if, when and how AI can be used for automated identification of individuals and differentiating between the identification of an individual vs the tracing and tracking of an individual, and between targeted surveillance and mass surveillance, will be crucial for the achievement of Trustworthy AI.*** *The application of such technologies must be clearly warranted in existing law. Where the legal basis for such activity is "consent", practical means must be developed which allow meaningful and verified consent to be given to being automatically identified by AI or equivalent technologies. This also applies to the usage of "anonymous" personal data that can be re-personalised*.[110]

90. Additionally, in June 2019 the Expert Group published *Policy and Investment Recommendations for Trustworthy AI* (**Recommendations**), comprising of 33 recommendations addressed to EU institutions and Member States. As part of its recommendations regarding appropriate governance and regulation, it recommended

[109] High-level Expert Group of Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (8 April 2019) <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.
[110] Ibid 33-4 [emphasis added].

that AI systems should be continuously evaluated about whether they generate risks that are not adequately addressed by existing legislation. To this end, the EU Expert Group specifically recommended that:

> *individuals should not be subject to unjustified personal, physical or mental tracking or identification, profiling and nudging through AI powered methods of biometric recognition, including facial recognition, and exceptional use of such technologies, such as… facial recognition. Exceptional use of such technologies, such as for national security purposes, must be evidence based, necessary and proportionate, as well as respectful of fundamental rights.*[111]

91. In July 2019, the incoming European Commission President expressed commitment in the first 100 days in office to 'put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence'.[112] In August 2019, it was reported that the European Commission is planning to legislate regulations that would give EU citizens' rights over their biometric information in the form of matching their face to their identity. It is reported that the plan is to limit the indiscriminate use of facial-recognition technology by private companies, police and security authorities and ensure citizens know when facial recognition data is used, with any exceptions tightly circumscribed.[113] It has been reported that the EU wants to write legislation to 'set a world-standard for AI regulation' with 'clear, predictable and uniform rules...which adequately protect individuals' by bringing facial-recognition technologies under the General Data Protection Regulation.[114] It is understood that any prospective legislation would build on recommendations made in June by the EU Expert Panel, where it suggested new rules were necessary to inform individuals when they were being targeted or under mass surveillance.[115]

92. The Law Council has previously raised the concern that the line between legitimate and proportionate uses of an interoperability hub for an open system, and illegitimate and disproportionate uses, should be clearly defined and assured by law. In the view of the Law Council, the need for this this clearly defined, legislated line is even more critical given the increase in the use of facial recognition technology integrated with the use of CCTV in Australia.

93. The Law Council considers that this legislation should entrench the principles that:

    (a) this line will not creep without careful foresight of consequences and an engaged public debate about why that creep is justified; and

    (b) the stability of the line will be maintained through operation of the provisions of the legislation itself, not just through anticipated operation of Ministerial

---

[111] High-level Expert Group on Artificial Intelligence, *Policy and Investment Recommendations for Trustworthy AI* (26 June 2019) 40 [28.1].
[112] Ursula von der Leyen, Candidate for President of the European Commission, 'Political Guidelines for the Next European Commission 2019-2014 (16 July 2019) <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf>.
[113] Adam Smith, 'Report: EU Commission To Clamp Down on Facial Recognition', *PC Mag News* (online, 23 August 2019) <https://www.pcmag.com/news/370336/report-eu-commission-to-clamp-down-on-facial-recognition>; 'EU Plans Strict Limits for Facial Recognition Technology', *The Irish Times* (online, 22 August 2019) <https://www.irishtimes.com/business/technology/eu-plans-strict-limits-for-facial-recognition-technology-1.3993782>.
[114] Ibid.
[115] Adam Smith, 'Report: EU Commission To Clamp Down on Facial Recognition', *PC Mag News* (online, 23 August 2019) <https://www.pcmag.com/news/370336/report-eu-commission-to-clamp-down-on-facial-recognition>.

discretion, ethical frameworks applicable to a diverse range of Federal, State and Territory government agencies.

94. For the Law Council's broader position and recommendations on the development of an Australian ethics framework for AI, the Law Council refers the Committee to its submission from June 2019 to the Department of Industry, Innovation and Science on *Artificial Intelligence: Australia's Ethics Framework.*[116]

[116] Law Council of Australia, Submission to the Department of Industry, Innovation and Science, *Artificial Intelligence: Australia's Ethics Framework* (28 June 2019) <https://www.lawcouncil.asn.au/resources/submissions/artificial-intelligence-australias-ethics-framework>.