Australian Council
for Civil Liberties

PJCIS Inquiry

Identity-Matching Services Bill 2018

and

The Australian Passports Amendment (Identity-Matching Services) Bill 2018

***A joint submission from**:*
NSW Council for Civil Liberties
Liberty Victoria
Queensland Council for Civil Liberties
South Australian Council for Civil Liberties
Australian Council for Civil Liberties

21/3/2018

1. The councils for civil liberties across Australia (New South Wales Council for Civil Liberties, Liberty Victoria, Queensland Council for Civil Liberties, South Australia Council for Civil Liberties and the Australian Council for Civil Liberties) are grateful for the opportunity to make this submission to the inquiry by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into *The Identity-Matching Services Bill 2018* and *The Australian Passports Amendment (Identity-Matching Services) Bill 2018.*

2. These Bills arise from COAG decisions made last year in relation to national security. As part of these, on 5 October 2017, Federal, State and Territorial leaders agreed to establish a National Facial Biometric Matching Capability and signed the Intergovernmental Agreement on Identity Matching Services (*IAIMS*).

3. The CCLs have broad concerns in relation to these Bills. This submission focusses on concerns in relation to specific provisions within the Bills. It is our intention to submit a brief supplementary submission setting out our more fundamental concerns.

IDENTITY-MATCHING SERVICES BILL 2018

4. *The Identity-matching Services Bill 2018* (the IMS Bill) will facilitate the exchange of identity information between the Commonwealth and State and Territory governments, pursuant to the IAIMS.
5. The purpose of the Bill is to collect, share and match identity information to identify people who are suspects or victims of terrorist or other criminal activity; prevent the use of fake or stolen identities; and for the purposes of protective security, community safety, road safety and identity verification. Agencies in all jurisdictions will be able to use identity matching services, for example, to access passport and driver licence images.
6. The CCLs have a number of concerns this Bill .

Rules and oversight

7. Identification information includes, in s.5(1)(n) "any information that is prescribed by the rules and relates to the individual." Identity-matching service includes, in s.7(1) (f):

> "a service prescribed by the rules that:
>
> *i.* involves the collection, use and disclosure of identification information; and
>
> *ii.* involves the interoperability hub or the NDLFRS."

8. Before making rules prescribing information for the purposes of s.5(1)(n) and s.7(1)(f), the Minister must consult the Human Rights Commissioner and the Information Commissioner. The OAIC is underfunded and, when that is coupled with a general lack of legislative will to protect privacy, it's doubtful whether the Commissioners' advices would be accepted.

9. As in the UK, a biometrics commissioner should be established who can respond to the collection, use and sharing of biometric information.[1]

10. S.30 permits the Minister to make rules as permitted by the Act, or necessary or convenient to giving effect to the Act. S.30(2) states that the rules may not do certain things. However, the list of exclusions is limited.

11. Making rules prescribing such important decisions means that many administrative processes are being made outside the legislative framework. It is well accepted that the rules which have a significant impact on individual rights and liberties should be included in the primary legislation.[2]

---

[1] Mann, Monique; Smith, Marcus --- "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" [2017] UNSWLawJl 6; (2017) 40(1) University of New South Wales Law Journal 121

< http://www.austlii.edu.au/au/journals/UNSWLJ/2017/6.html> (*Mann & Smith)*

[2] https://www.alrc.gov.au/publications/justifications-delegating-legislative-power-0

12. By deferring these important decisions to delegated legislation and eliminating barriers to data sharing, the level of scrutiny of these processes is reduced, because there is no parliamentary oversight.
13. Rules that involve the collection, use and disclosure of identification information have the potential to impact rights and liberties, particularly as the Bill exempts agencies from compliance with APPs 2, 3 and 6.
14. Relevant examples of provisions that should not be delegated to these rules are those that:

    - infringe personal liberty;
    - interfere with freedom of movement;
    - interfere with freedom of speech;
    - restrict access to the courts;
    - interfere with the course of justice;
    - deny procedural fairness to persons affected by the exercise of public power;
    - give executive immunities a wide application;
    - unduly make the rights and liberties of citizens dependent upon administrative decisions which are not subject to review of their merits by a judicial or other independent tribunal; and
    - involve significant questions of policy including significant new policy or fundamental changes to existing policy;
    - procedural matters that go to the essence of the legislative scheme; and
    - provisions creating statutory authorities.

Recommendation 1

The CCLs recommend:

i) Consideration be given to the establishment of a biometrics commissioner as in the UK to respond to the collection, use and sharing of biometric information.

ii) In both cases of identification information and identity-matching services, the Privacy Commissioner should also be consulted (as that position is at present distinct from Information Commissioner).

iii) An independent statutory agency, with broad oversight of and review powers in relation to the operations of the identity matching services should be established and report annually to Parliament.

iv) S30.2 should be amended to ensure that rules which will have adverse effects on individual liberties or rights cannot be made by the Minister.

Non-government entities and consent

15. S.7(2) provides that the Minister has a discretion to make rules in relation to a request from a local government authority or non-government entity, for the purpose of using the identity matching service to verify an individual's identity. s10 (2)(d) permits a non-government entity to access the FVS. In both cases, certain conditions in s.7(3) need to be met.

16. Access by non-government entities is of particular concern as there is very little detail in the Bill about who will be able to access this information and for what identification purposes.

17. It is not clear whether some or all of these entities are entrusted persons for the purposes of the offences of disclosure in s.21(4). Also, not all non-government entities are subject to the Privacy Act 1988, for example, small businesses. Further, the Bill specifically permits the collection of sensitive information (s17(1)). [3]

18. One of the conditions in 7(3)(b), is that the individual has given consent. The necessity for information sharing in the Bill is justified as being in the legitimate interest of the government and that in such cases consent of the affected individual is not required.[4] In all cases, consent should be valid, free and voluntary. This is quite often not the case

[3] as defined in the Privacy Act 1988

[4] Identity-Matching Services Bill 2018, Explanatory Memorandum, Statement of Compatibility with Human Rights atp.40

when no real choice or alternative is offered and there is little or no opportunity to opt out.

19. The IAIMS stated that a private/non-government entity must have a legislative basis or authority to access the FVS. Instead, s.7(3)(a) of the Bill states that:

    "verification of the individual's identity is reasonably necessary for one or more of the functions or activities of the local government authority or non-government entity."

20. This is a watered-down version of what was promised. Under the broad purpose of verifying the identity of an individual (s.6(8)) the local government might, for example, integrated with CCTV, use the services to issue parking tickets.
21. Some businesses in the UK are using 'Facewatch' to share CCTV images with police and being notified of suspected shoplifters; demonstrating the use pre-emptive identification of alleged future criminals.[5]

Recommendation 2

The CCLs recommend:

i) Non-government entities should not be allowed access to the proposed identity-matching services

ii) S.7(3)(a) of the Bill should be amended to: delete the reference to '*non-government entities*' and the word *'reasonably'* and to include a requirement that the relevant function or activities cited by a local government agency are tightly aligned with a community protection activity as defined in S6 subsection (2), (3), (4), (5), (6), (7).

iii) Valid consent by an individual must be predicated on sufficient information on the use of the data, being provided to the affected individual.

[5] 'Facewatch "Thief Recognition" CCTV on Trial in UK Stores', BBC News (online), 16 December 2015 <http://www.bbc.com/news/technology-35111363> .in Mann & Smith

Function creep

22. S.17 permits the collection of sensitive information. S.18 permits the use and disclosure of identification information, including sensitive information. Both are therefore authorised for the purposes of Australian Privacy Principles (*APP*) 3 & 6, respectively.
23. There are specific exceptions to the definition of identification information in the Bill, which exceptions include racial or ethnic origin, health information and genetic information (s.5(2)). However, incidental collection, use or disclosure is permitted (s.5(3)).
24. The abuse of such incidental information is possible should the Minister prescribe rules under 5(1)(n). The risk exists that information provided for a specific purpose will subsequently become available for secondary purposes for which consent was not obtained. S28(2) provides that the report must not unreasonably disclose personal information about an individual. No identified data should be disclosed for report purposes.

Recommendation 3

The CCLs recommend:

i) The collection, use or disclosure of excluded, incidentally collected identification information should not be permitted for discriminatory targeting and profiling purposes.
ii) Further use or disclosure of de-identified information collected in the course of identity-matching services, should be prohibited.
iii) Unwarranted function or 'purpose' creep should be closely monitored and reported on annually by the proposed oversighting body.

Privacy measures

25. The acts and practices of some Australian Government agencies, including the

intelligence agencies, are completely exempt from the Privacy Act.[6] The IAIMS stressed that the Commonwealth would be guided by the principle of maintaining "robust privacy safeguards", developed in consultation with Federal and State Privacy Commissioners. [7] Participating agencies were to "implement appropriate security and access controls".[8]

26. None of these privacy safeguards are in the Bill. Consideration needs to be given in particular to safeguards for minors, the elderly and other vulnerable individuals.

27. The IAIMS required that all reasonable steps be taken to notify applicants, obtaining new or renewing driver's licences, that their personal information would be collected by the road agency for the purposes of biometric matching. This is not in the Bill.

28. The IAIMS also promised a public register of arrangements for sharing identity information. This is not in the Bill.

Recommendation 4

The CCLs recommend that the Bill –or the Explanatory Memorandum - be amended to explicitly incorporate measures proposed by IAIMS to ensure 'robust privacy safeguards' and 'security and access controls' including:

i) audit trails, independent vulnerability tests and security reviews, and mechanisms for responding to public complaints.
ii) clear safeguards for vulnerable individuals
iii) all reasonable steps to notify applicants for driver's licences, that their personal information will be collected for the purposes of biometric matching.
iv) a public register of arrangements for sharing identity information.,

[6] S7 Privacy Act 1988
[7] Ibid clause 2.1(a)
[8] Ibid clause 2.1 (b)

Legitimate Aim

29. One effect of the Bill is that disclosure of a person's identity is authorised for the purposes of APP 2.[9] To the extent that this right is restricted, any interference must be "necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available."[10] The limitation must be more than useful, reasonable or desirable.[11]
30. Non-digital tools for national security and law enforcement are downplayed by government. It is, therefore, difficult for the public to measure whether restrictions on privacy and anonymity are justified, compared to any perceived benefits, and whether there is a less intrusive method to achieve the desired end.[12] Since the restriction will have "a broad impact on individuals who pose no threat to a legitimate government interest, the state's burden to justify the restriction" is high.[13]
31. Furthermore, the limitation should be subject to regular review by an independent and impartial statutory authority. The Bill provides for a review of its operation by the Minister only within 5 years of its commencement (s.29). Annual reporting to the Minister provides mostly statistical information. (see Recommendation 1(iii))

Recommendation 5

The CCLs recommend:

i) The public should be informed of possible meaningful alternatives to collection of the identity information for the purposes of law enforcement and national security. All government agencies and non-government entities should be providing those practical, alternative means of accessing services; in the interests of proportionality

[9] APP 2 , Schedule 1 Privacy Act 1988 permitting individuals to have the option of not identifying themselves, or of using a pseudonym.
[10] Office of the United Nations Commissioner for Human Rights, "The Right to Privacy in the Digital Age" UN Doc A/HRC/27/37 (2014), paragraph 23
[11] Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" UN Doc A/HRC/29/32 (2015), paragraph 34
[12] Ibid paragraph 36
[13] Ibid paragraph 35

and to preserve the right to anonymity so that the individuals do not have to compulsorily participate.

ii) Law enforcement, authorities or non-government entities that may otherwise have authorised access, should be monitored; for example, using audit trails, annual compliance audits and a system of appropriate notifications. [14]

Data Security

32. The recent hacking of a national security contractor, has emphasised how easily the security of systems may be compromised and personal information acquired for illegal purposes. [15] Although identity theft is a threat to privacy when it involves the theft of someone's identity, new systems inherently increase the possibility of covert or illegal collection, storage and processing of sensitive material.

33. Facial identity information is unique data tied to an individual's biological existence. It cannot be replaced, as one might a credit card and the potential exists for an individual to be compromised for life. [16] Spoofing attacks and fraudulent or unauthorised infiltration are major issues.[17]

34. IAIMS promised use of appropriate cryptographic technology and organisational, procedural measures in the processing, transmission and storage of biometric information.

---

[14] IAIMS, Op Cit, paragraphs 9.9 & 11.7(c).

[15] Conifer, D (10 October 2017) "Defence contractor's computer system hacked, files stolen, cyber security report reveals" ABC News, accessed 17 Nov 2017, <mobile.abc.net.au/news/2017-10-10/defence-contractors-fles-stolen-in-hacking:-security-report/9032290>

[16] Article 29 Data Protection Working Party- European Commission "Opinion 3/2012 on developments in biometric technologies" 00720/12/EN , retrieved 7 October 2017 < http://ec.europa.eu/justice/data-protection/index_en.htm>, (*DPWP*) p.9; Froomkin, A.M. (2000) "The Death of Privacy?" Stanford Law Review, Vol 52, No.5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? Pp 1461-1543 at p.1495

[17] DPWP, Op Cit, paragraph 5.3.2

Recommendation 6

The CCLs recommend:

i) Effective oversight and implementation of technical protection against accidental or unauthorised interception, access or disclosure of information; and embedding of privacy, including but not limited to:
    a) the automatic deletion of raw data after the template is calculated.
    b) authentication of data which is not secret, such as facial features, with other lockable or changeable credentials to insure against spoofing and fraudulent mismatching, to determine whether biometric data is genuine and still connected to a natural person.
    c) the processing of data which allows for the extraction of multiple and independent biometric templates from the same source in order to replace them in the case of a data breach.

ii) No exemptions should be made to data breach notification as the loss of directly identified biometric data seriously compromises the capacity of affected individuals to be able to defend themselves against any future identity challenges

Accuracy

35. It is difficult to produce completely error-free results with biometric identity information which may be due to differences at the time of data acquisition, like lighting and the equipment used. To accommodate for these factors, technicians generate a certain tolerance, decreasing systems' accuracy. As an example, the FBI's algorithm has a tolerance of, at least, 15%.[18]
36. Inconsistent human interpretation, or mis-description, increases the identity error margin and consequent risk of inaccurate identifications.[19] Since the consequence of an individual being falsely accepted or rejected is potentially serious, accuracy and reliability needs to be constantly assessed.[20]

---

[18] Solon, O (27 March 2017) "Facial recognition database used by FBI is out of control, House committee hears" The Guardian, , accessed 18 November 17,https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports

[19] White D, Dunn JD, Schmid AC, Kemp RI (2015) " Error Rates in Users of Automatic Face Recognition Software". *PLoS ONE*10(10): e0139827. https://doi.org/10.1371/journal.pone.0139827

[20] ALRC Report 108, Op Cit, paragraph 9.71

Recommendation 7

The CCLs recommend that the Bill – or the Explanatory Memorandum- should be amended to:

i) explicitly require each agency to take robust steps "to maintain the accuracy, integrity and availability of ….information including measures to ensure facial images are of appropriate quality for biometric matching." [21]

ii) specify that identity matching not be the sole basis for identifying an individual for evidentiary purposes.[22]

Data minimization

37. The Commonwealth first announced the National Facial Biometric Matching Capability in 2015. Its own Privacy Impact Assessment warned that more information would be collected than necessary (including facial images from data bases) and not enough would be done to protect that data[23].

38. The IAIMS stated that the Face Recognition Solution "will not hold information that is not reasonably necessary to support identity matching"[24].

Recommendation 8

The CCLs recommend:

i) The principle of data minimisation should be upheld so that only required information is processed, stored and transmitted.

ii) The data retention period should be no longer than is necessary for the purposes for which the data is collected or for which it is to be further processed.[25] Data not needed anymore for processing should be automatically destroyed.

---

[21] IAIMS, Op Cit, clause 2.1(d)

[22] Ibid clause 2.1 (f)

[23] Lauder, S. (17 Dec 2015) "The Capability: Government's national facial recognition plan raises privacy concerns" ABC News, accessed 7 October 2017, <http://www.abc.net.au/news/2015-12-17/governments-facial-recognition-system-sparks-privacy-concerns/7035980>

[24] IAIMS, Op Cit, clause 6.16(a)

AUSTRALIAN PASSPORTS AMENDMENT (IDENTITY-MATCHING SERVICES) BILL 2018

39. The purpose of this Bill is set out in the Explanatory Memorandum:

> *'This Bill amends the Australian Passports Act 2005 (Passports Act) to provide a legal basis for ensuring that the Minister is able to make Australian travel document data available for all the purposes of, and by the automated means intrinsic to, the identity-matching services to which the Commonwealth and the States and Territories agreed in the Intergovernmental Agreement on Identity Matching Services (IGA), signed at a meeting of the Council of Australian Governments on 5 October 2017'.* [26]

40. The CCLS want to reference two areas of concern with this Bill.

Rules

41. S 46(da) provides an additional purpose for the disclosure of personal information by the Minister, of a kind specified in a Minister's determination.

42. Making rules prescribing such important decisions means that many administrative processes are being made outside the legislative framework. As noted in our comments on the IMS Bill ((paragraphs 9-11), It is well accepted that the rules which have a significant impact on individual rights and liberties should be included in the primary legislation. By deferring these important decisions to delegated legislation and eliminating barriers to data sharing, the level of scrutiny of these processes is reduced. As noted in our comments on the IMS Bill (paragraphs 9-11).

---

[25] DPWP Op Cit, paragraph 3 p.10
[26] Australian Passports Amendment (Identity-Matching Services) Bill 2018. Explanatory Memorandum p1

Recommendation 9

The CCLs recommend that S46(da) is amended to specify that provisions impacting individual rights and liberties should be included in the Act, not in rules determined outside the legislation.

Ministerial decision-making by computer

43. S.56A provides that the Minister may arrange for use of computer programs for making decisions, exercising power, complying with obligations – or doing '*anything else related to making a decision or exercising a power or complying with an obligation'*.

44. Australian law has explicitly allowed, for some time, computers to make important decisions previously made by ministers or staff. There is little public knowledge as to what decisions are being entrusted to computers.

45. Australian Federal Court justice Melissa Perry noted in a 2014 speech on the topic of automated decision-making in government that "[i]n a society governed by the rule of law, administrative processes need to be transparent and accountability for their result facilitated".[27]
46. Incorrect or unfair decisions and lack of procedural fairness are a danger when computers replace a human decision maker. The Centrelink Robodebt fiasco demonstrated the significant harm that could be caused to individuals. In that case the onus of proof was also reversed, so that individuals had to prove they were entitled to receive the benefits being claimed back.[28]
47. The CCLs have strong concerns about this provision. If it is to be enacted, it is essential that the range of 'Ministerial' decisions that are being made by computers and the underpinning data used to generate these decisions are publicly available.

---

[27] http://www.abc.net.au/news/2017-07-21/algorithms-can-make-decisions-on-behalf-of-federal-ministers/8704858

[28] http://www.abc.net.au/news/2017-07-21/algorithms-can-make-decisions-on-behalf-of-federal-ministers/8704858

48. It is also essential that strong procedural fairness criteria are built into the computer programs and that effective and easily accessed appeal process are in place.

Recommendation 10

The CCLs recommend:

i) S 56A should be deleted from the Bill

Or failing that:

ii) If S.56A is enacted, any delegation of the minister's decision-making process to computer programs should ensure strong in-built procedural fairness criteria and effective and easily accessed appeal processes are in place.

Concluding comments

41. The CCLs hope this short submission assists the Committee in its review of these Bills.

42. This submission was written on behalf of the Joint Councils for Civil Liberties by Michelle Feinstein (Convenor of the NSWCCL Privacy Action Group) with input from Stephen Blanks (President NSWCCL) and Michael Cope (President Queensland CCL.)

Therese Cochran

Secretary

NSW Council for Civil Liberties

Contact in relation to this submission
Dr Lesley Lynch Vice President
NSWCCL

Lesley.lynch@nswccl.org.au ; mob 0416 497 508