Electronic Frontiers
AUSTRALIA

W www.efa.org.au
E email@efa.org.au
@efa_oz

27 September 2019

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

By Email: pjcis@aph.gov.au

Dear Secretary,

RE: Review of the *Identity-matching Services Bill 2019* and the *Australian Passports Amendment (Identity-matching Services) Bill 2019*

We appreciate this opportunity to make submissions in relation to the *Identity-matching Services Bill 2019* ("**the Bill**") and the *Australian Passports Amendment (Identity-matching Services) Bill 2019* (collectively, "**the Bills**"). We additionally thank the Committee for the extension of time for this submission to be prepared and submitted by 1 October 2019.

EFA's submission is contained in the following pages.

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights. EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

[redacted]

Angus Murray
Chair of the Policy Committee
Electronic Frontiers Australia

Introduction

1. As the Committee would be aware, the Bills originate from the Intergovernmental Agreement on Identity Matching Services agreed by the Coalition of Australian Governments in October 2017 which incepted the ominously named "National Facial Biometric Matching Capability" ("**the Capability**"). As the Committee may be aware, EFA has been opposed to the Capability from its inception.

2. We maintain our position expressed on 4 October 2017, being that:

> *EFA considers this to be just the latest incremental (and probably irreversible) increase in temperature to the pot that's slowing boiling the privacy rights of Australians. Meanwhile, we still don't have an enforceable right to privacy or a civil course of action to seek redress for serious invasion of privacy.*
>
> *Even the Privacy Impact Assessment from the Attorney General's Department notes the potential massive scope of this proposal, saying that the "scope of NFBMC (National Facial Biometric Matching Capability)... seems very broad and which, with the inclusion of service delivery, seems to anticipate facial biometrics being used in the context of almost all government activities".*[1]

3. The Bills were previously introduced in 2018 and was subject to an inquiry before the Committee which lapsed with the dissolution of the House of Representatives on 11 April 2019.

4. The Bills have been introduced in identical terms and, with respect, the criticisms of the Bills made in numerous submissions in 2018[2] remain accurate and valid.

5. In our submission, Australians ought to be afforded the benefit of a base-line safeguard for human rights protection in the form of a Federal enforceable human rights framework *before* any further legislation is passed that has potential to impact on Australian's human rights.

6. On the above basis, and for the reasons contained in this submission, EFA submits that the Bills should be rejected and, in the event this submission is not accepted, we have proposed recommendations that serves as the minimum requirements to bring the Bills to an acceptable standard.

Submissions and Recommendations

7. At the outset, it is important to understand that the information sought to be collected, used and disclosed by operation of the Bill is biometric information that falls within the definition of

---

[1] See: https://www.efa.org.au/2017/10/04/national-facial-recognition/.
[2] See for example; Submission Nos.: 1 (Future Wise and the Australian Privacy Foundation), 3 (Queensland OIC), 4 (Victorian OIC) 9 (Joint Councils for Civil Liberties), 10 (Queensland Council for Civil Liberties), 11 (Human Rights Commission) and 16 (Human Rights Law Centre).

sensitive information[3]. It is relevant to note that Item 42 of Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* ("**the EM 2012**") which introduced biometric information into the *Privacy Act 1988* ("**the Privacy Act**") provided that:

> *Item 42 will amend the definition of sensitive information in subsection 6(1) of the Privacy Act by adding references to biometric information and biometric templates. The inclusion of these two paragraphs will implement the Government's response to ALRC Recommendation 6-4. The Government agreed with the ALRC that biometric information had similar attributes to other sensitive information and it was therefore desirable to provide it with a higher level of protection.*[4]

8. The EM 2012 continued to make clear that:

> *As noted above, that definition now applies to agencies, and includes biometric information and biometric templates. The general rule is that sensitive information can only be collected by agencies or organisations where the collection meets the criteria outlined in APP 3.1 and APP 3.2 and where the individual has consented to the collection.*[5]

9. While we accept that the Privacy Act and the Australian Privacy Principles do allow for collection of sensitive information without consent, such collection may only occur where an enforcement body reasonably believes that the collection is reasonably necessary for the entities functions or activities (or related activities in the case of the Home Affairs Department).

10. Despite our critique of the Capability when it was first introduced (and notwithstanding the comments made in the Privacy Impact Assessment that "[it] seems very broad and which, with the inclusion of service delivery, seems to anticipate facial biometrics being used in the context of almost all government activities"), the Explanatory Memoranda for the Bills provide an almost open-ended list of purposes being:

    a. Preventing identity crime;
    b. General law enforcement;
    c. National security;
    d. Protective security;
    e. Community safety;
    f. Road safety; and
    g. Identity verification[6].

11. It is also clear that the scope of the Bills can (and likely will) be crept with the Hon Peter Dutton MP, Minister for Home Affairs stating in his second reading that:

---

[3] Section 6 of the *Privacy Act 1988*.
[4] See: Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* at Page 62.
[5] Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* at Page 76.
[6] See: Explanatory Memorandum to the *Identity-matching Services Bill 2019* at Page 2.

> "*The identity-matching services will also make it harder for persons to obtain driver licences in false identities in an attempt to avoid traffic fines, demerit points or licence cancellations.* ***This will improve road safety by increasing the detection and prosecution of these offences and deterring dangerous driving activity***"[7].
>
> (our emphasis)

12. It is our view that the scope of the Bills dramatically and inappropriately exceed Australian's reasonable expectations to human rights protection, including the rights to privacy and association.

13. Indeed, the likely effect of Bills is readily comparable to the Australia Card postulated in the *Australia Card Bill 1986* which was introduced in 1986, failed to pass the Senate and was subsequently abandoned by Government in 1987. In our submission, the only great difference between the Australia Card and the Capability proposed by the Bills is the interposition of a "hub" to manage queries - a minor technological differential to the original scheme that was appropriately shut down in 1986.

14. In our submission, the Bills produce a manifestly excessive power with little effective safeguard to abuse and scope creep.

    Recommendation One: The Bills be rejected.

15. We have provided further and more specific critique of the Bills in the following pages with the following recommendations being made should the Bill proceed.

    Recommendation Two: The Bills should not proceed in their current form.

    Recommendation Three: Clauses 5(1)(n) and 7(1)(f) of the Bill be removed as new types of identification information and new types of identity-matching services ought not merely be subject to prescription by the Minister.

    Recommendation Four: A Biometrics Commissioner, akin to the UK Biometrics Commissioner ought to be established to oversee and review the operation of the Capability.

    Recommendation Five: There ought to be greater reporting and oversight of the Capability.

    Recommendation Six: Non-government entities should be expressly prevently from access to the Capability.

---

[7] Commonwealth, Parliamentary Debates, House of Representatives, 7 February 2018, *Hansard* at [487] (the Hon Peter Dutton MP).

Recommendation Seven: The public ought to be informed as to the operation of the Capability.

Recommendation Eight: Australian citizens ought to be entitled to transparent access to personal and/or sensitive information held within the Capability.

Recommendation Nine: Increased Data Breach Notification requirements ought to be implemented in specific relation to information collected, used or disclosed by operation of the Capability.

Recommendation Ten: The Capability ought not be the sole basis for identifying an individual for evidentiary purposes.

Recommendation Eleven: Section 56A of the *Australian Passports Act 2005* be amended:

> **to include express provision for reporting on the use of computer programs to make a decision; and**
> **to expressly enable merits review of any substituted decision pursuant to s. 56A(3)**

16. We have expressed our reasons for each of the abovementioned eleven (11) specific recommendations as they respectively apply to the Bills.

Identity-matching Services Bill 2019

Recommendation One: The Bills be rejected.
Recommendation Two: The Bills should not proceed in their current form.

17. While we respectfully appreciate the potential intention behind the Bills being an efficient means to improving policing in Australia, the underlying biometric technology needs to be understood and improved before such a scheme could properly be introduced. It is also difficult to accept that Australians ought to forego their ability to consent to the collection, use and disclosure of their personal and sensitive information on the basis of justification that law enforcement *might* benefit from this system (as opposed to justification based upon evidence of *actual* shortfalls within the current legislative framework).

18. In our submission, the Bills are merely being introduced to make policing easier and shifting burdens onto everyday Australians. In our view, this is wholly inappropriate and inconsistent with the regulation of biometrics in other jurisdictions.

19. For example, the Swedish Datainspektionen recently fined a public school in Anderstorps the sum of SEK200,000 for its use of a pilot biometric facial recognition project intended to

increase the efficiency of taking class registers[8]. Of most relevance to the Bills was the finding that the project offended Article 5 of the *General Data Protection Regulation* ("**GDPR**"), being the requirement that personal data shall be collected for specific, explicitly stated and legitimate purposes and not later used in a manner incompatible with these purposes.

20. It is incongruous to accept that a person who obtained a drivers license in, say, 2005 would have consented to that license being used for any purpose other than roadside verification of entitlement to operate a motor vehicle and voluntarily disclosing identity to third parties where such proof was necessary.

21. It is also relevant that Australia takes careful notice of the implementation of biometric databases and identification services occurring elsewhere in the World. For example, it is our respectful submission that the GDPR and example of the Swedish Datainspektionen's position regarding the use of biometrics ought to be preferred over the ubiquitous and Orwellian approach being taken in China[9].

22. EFA respectfully submits that the Bills are yet another example of Government rushing to achieve a non-transparent end to broad goal without proper and complete regard to the reasonable expectations of Australian citizens.

Recommendation Three: Clauses 5(1)(n) and 7(1)(f) of the Bill be removed as new types of identification information and new types of identity-matching services ought not merely be subject to prescription by the Minister.

23. It is trite that biometric analysis be described as a new and emerging technology. There are a variety of emerging biometric identification methods, such as identification via brain waves and neural activity[10], that, under the Bill's present form, could be included merely via prescription.

24. It is our respectful submission that biometric technology, and the potential ancillary consequences that follow biometric analysis and discrimination, ought to be approach with caution and consideration and that the legislature ought to present a proper basis for any new types of identification information or matching services with proper debate regarding same prior to their inclusion into this framework.

---

[8] See: https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/
[9] See for example: https://www.abc.net.au/news/2018-03-20/china-deploys-ai-cameras-to-tackle-jaywalkers-in-shenzhen/9567430.
[10] See for example: Xiang Zhang, Lina Yao, Salil S. Kanhere, Yunhao Liu, Tao Gu, and Kaixuan Chen. 2017. MindID: Person Identification from Brain Waves through Attention-based Recurrent Neural Network. ACM J. *Comput. Cult. Herit.* 9, 4, Article 39 (March 2017).

Recommendation Four: A Biometrics Commissioner, akin to the UK Biometrics Commissioner ought to be established to oversee and review the operation of the Capability.

25. As the Committee would be aware, the United Kingdom Biometrics Commission was established under the *Protection of Freedoms Act 2012* in response to the decision in *S and Marper v United Kingdom*[11].

26. In our submission, should the Bills be progressed, Australia ought to create a specific statutory Biometrics Commissioner to oversee the collection, retention, use and disclosure of biometric information with reporting obligations regarding said oversight[12]. We further submit that a Biometrics Commissioner is necessary to ensure that the collection, retention, use and disclosure of biometric information is not disproportionate to the reasonable belief and reasonable necessary operation of law enforcement bodies.

Recommendation Five: There ought to be greater reporting and oversight of the Capability.

27. We appreciate that the Bill incorporates an annual reporting obligation; however, we submit that this obligation ought to be extended to include system failures (see Recommendation Twelve below) and that Facial Verification Service users be specifically named within the report (notwithstanding Recommendation Six).

Recommendation Six: Non-government entities should be expressly prevented from access to the Capability.

28. There is no justification for the Australian Government to enable access to the Capability to any other body.

29. Whilst we appreciate that the Capability will operate as a "hub", it is unacceptable for this platform to be made available outside of clearly defined (which we respectfully submit is not the case in any event) law enforcement purposes.

Recommendation Seven: The public ought to be informed as to the operation of the Capability.

30. The Capability has significant ramifications for the interaction between government, law enforcement and citizens. As abovementioned, it is highly improbable to suggest that the historic acquisition of a driver's license involved consent to the Capability and a clear campaign ought to be run prior to the Bills passing to ensure that the Australian public is properly and objectively informed as to the operation, risks and benefits of the Capability.

---

[11] [2008] ECHR 1581.

[12] See: Monique Mann and Marcus Smith, 'Automated facial recognition technology: Recent developments and approaches to oversight' (2017) 40(1) *University of New South Wales Law Journal* 121, 139 - 141.

31. It is also important to ensure that the regulatory framework for the operation of this platform (whether overseen by the Office of the Australian Information Commissioner and/or a Biometrics Commissioner) is appropriately funded to oversee the function of the Capability and engage in public education[13].

Recommendation Eight: Australian citizens ought to be entitled to transparent access to personal and/or sensitive information held within the Capability.

32. Australians ought to be able to query and receive transparent information regarding the collection, use and disclosure of their personal and sensitive information in relation to the Capability. In our submission, this is a fundamental right that ought to be enjoyed by all Australians and, should the Bills progress, complete transparency ought to be recommended by the Committee.

Recommendation Nine: Increased Data Breach Notification requirements ought to be implemented in specific relation to information collected, used or disclosed by operation of the Capability.

33. Whilst we appreciate the intention underlying an interposed "hub" for exchange and verification of biometric information, it is our view that a real and serious risk of data breach (either by operator error or malicious attack) exists in relation to the Capability.

34. It is incumbent on government to ensure that Australian's are protected and that the Capability does not create an unintentional consequence of its own existence. Namely, we are concerned that the collection, use and disclosure of personal and sensitive information for the purpose of "protecting Australians against identity theft" may correspondingly become the very vehicle by which Australian's identities are compromised.

35. This is a risk that will be present with any digital platform and, in our submission, Australians ought to be made promptly and completely aware of any issue with the operation of the Capability, including any actual or potential data breach or unlawful access.

36. We make this recommendation with the intention that the Minister for Home Affairs be required to table and make public a comprehensive annual report regarding the operation of the Capability and a candid account of its integrity and effect (including clear reporting regarding false-positive matching).

---

[13] Monique Mann and Marcus Smith, 'Automated facial recognition technology: Recent developments and approaches to oversight' (2017) 40(1) *University of New South Wales Law Journal* 121, 143 - 144.

Recommendation Ten: The Capability ought not be the sole basis for identifying an individual for evidentiary purposes.

37. An unfortunate consequence of the rapid adoption of technology by law enforcement has been that traditional policing has and is being replaced with technology solutions. It is our concern that the Capability will continue this trajectory.

38. Our submission posits this technology is not perfect[14] (and likely will never be perfect) and it should not become a *fait accompli* for law enforcement.

Australian Passports Amendment (Identity-matching Services) Bill 2019

Recommendation Eleven: Section 56A of the *Australian Passports Act 2005* be removed or otherwise amended:

to include express provision for reporting on the use of computer programs to make a decision; and
to expressly enable merits review of any substituted decision pursuant to s. 56A(3)

39. As the Committee would be aware, computerised decision making has caused significant issues in Australia with the most obvious example being (ongoing) the "RoboDebt" scandal[15].

40. In our submission, there are significant and serious issues that arise from computerised decision making including:

    a. The vexxed status of administrative law[16] in Australian in relation to the review of computerised (non-human) decisions;

    b. The application of advanced technologies, such as artificially intelligent systems, is not yet properly subject to an ethical framework[17];

    c. There has not been a consistent approach to the legislative's approach to the arrangement for use of computer programs across Australia law[18]; and

---

[14] It is relevant to note that a US Congressional Hearing received evidence that "*the algorithms that make the matches are wrong 15 percent of the time and are more likely to misidentify African-Americans*", see: https://www.9news.com.au/national/chris-uhlmann-pm-to-use-counter-terror-meeting-to-push-for-drivers-licence-photo-database/5a16558c-cd91-4c2f-8c9b-d9ae223c25e0; https://www.efa.org.au/2017/10/04/national-facial-recognition/.

[15] https://www.notmydebt.com.au/the-issue; https://www.theguardian.com/australia-news/2019/may/08/labor-not-revealing-position-on-robotdebt-scheme-despite-attacking-coalition.

[16] See: *Pintarich v Deputy Commissioner of Taxation* [2018] FCAFC 79 at [47] - [49] per Kerr J.

[17] Noting this is a subject under domestic and international consideration, see: https://ec.europa.eu/futurium/en/ai-alliance-consultation; https://tech.humanrights.gov.au/; https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/.

[18] Murray, A, *Computer Says No... but then what?* [online] Proctor Vol 39, No. 8 at Page 50, Available at URL: http://proctor.qls.com.au/?iid=165199#folio=50.

d. The threshold of "satisfaction" required to be formed by the Minister arguably invokes the principle enunciated in *Avon Downs*[19] and restricts review options.

41. Even more concerningly, a further consequence of the application of s. 56A of the *Australian Passports Amendment (Identity-matching Services) Bill 2019* is that the power to determine identify (in the instant circumstance vested with the Minister and operated by delegation) is divested from the executive and placed into the hands of technology service providers.

42. We strongly recommend that caution be taken in relation to the passing of power from the elected into the hands of the contracted, particularly where this occurs as regards advanced technologies that are not yet fully and comprehensively understood.

Conclusion

43. In summary, EFA recommends the rejection of the Bills and has made ancillary recommendations should our primary submission be rejected.

44. We consider that these submissions would be assisted by the Committee receiving oral evidence from EFA and confirm that we will be available to provide such evidence at the Committee's convenience.

45. We trust that these submissions are of assistance.

Please do not hesitate to contact Mr Angus Murray, Chair of Electronic Frontiers Australia's Policy Committee should you require any further information or assistance.

Yours sincerely,

Angus Murray
Chair - Policy Committee
Electronic Frontiers Australia

[19] *Avon Downs Pty Ltd v Federal Commissioner of Taxation* [1949] HCA 26.