Digital Transformation Agency
Australian Government

Via web: https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/submission-form

14 July 2021

Dear Sir/Madam

Re. Phase 2 consultation – Digital Identity Legislation

Introduction

Thank you for the opportunity to make a submission to Phase 2 of the public consultation on the proposed Digital Identity legislation, specifically with reference to the current Position Paper.

Who we are

This submission has been prepared by: Dr. Megan Prictor and Associate Professor Mark Taylor, researchers in health law and regulation at Melbourne Law School; and Gabby Bush, Program Manager, Centre for AI and Digital Ethics, the University of Melbourne. More information about individual authors is available on the University of Melbourne website.

The opinions in this submission are those of the named authors and should not be taken to represent the views of the University of Melbourne. The authors are happy to provide further clarification on any area of the submission.

Outline

This submission addresses several discrete elements of the Digital Identity Legislation Position Paper; namely automated decision making, the use of biometric information, data profiling, user consent, data breach notification and enforcement agency access.

1. Automated decision making

Section 6.5.3 of the Position Paper details the use of automated decision making without respect to the gravity of deploying these technologies.

1.1 Neutral or favourable outcomes

The Position Paper states that the automated decision-making will be "limited to either neutral or favourable outcomes to an individual," most likely 'yes' or 'no' decisions.

This statement is problematic due to the preconceived notion that any decision is neutral or the qualifier that it is favourable. The previous sentence states that the decisions would be "non-discretionary" which is contradictory to the idea that they would be "favourable."

Postal address:
Melbourne Law School, 185 Pelham Street, Carlton VIC 3053
Phone:
+61 3 9035 9644

Decision-making algorithms usually use a machine learning process that learn from typical decisions – meaning that the algorithm will learn to say yes/no based on a series of factors – but these factors will often lack nuance, which may end up excluding those with situations more complicated than the learnt factors. This is especially important in a case that the decision would either be a 'yes' or 'no' as this may block someone from receiving government assistance entirely.

1.2 Ethical use of automated decision-making

Current research shows that the most ethical deployment of automated decision-making requires a process of explainability and the ability to contest that decision. Section 6.5.3 does not detail what the algorithm will be or even explicitly what it will be used for. Will the code be open source? Will it be available for reverse engineering? Will the algorithm be explained it its entirety?

Furthermore, if the algorithm is deployed in the vague instances of this report, will there be the option for people to contest the outcome of the decision? If the outcome happens to *not* be favourable for the user, can the user argue for the reversal of the decision? What would the process be for this? Do users have the option not to use the algorithm if it has originally provided them with a non-favourable outcome?

2. Safeguards on biometric information

It is proposed to allow for random sampling of biometric information that has not yet been deleted to test and refine matching algorithms, and to inform anonymous aggregate reporting on biometric accuracy, subject to a number of conditions, including that this is done "pursuant to an ethics plan that considers human rights and privacy risks done in accordance with the TDIF rules" (7.4.2). It needs to be made clear the expectations of an "ethics plan" and the principles and process by which its adequacy would be assessed.

3. Restrictions on data profiling

It is proposed the Bill will prohibit Accredited Participants from collecting, using and disclosing information about a User's behaviour unless an exception applies (7.4.3). One of the proposed exceptions to the prohibition is where Accredited Participants de-identify data to create aggregate data. It would be a mistake to suggest or assume that the use of aggregate data poses no issues of significance to data subjects. Aggregate data may be used to associate characteristics to groups which may have implications for data profiling. The individual and group interests in aggregate data should be protected by effective controls over the purposes for which aggregate data may be used, in particular to ensure that any processing is in the Users' interests.

4. User consent and access to user history log

Section 7.4.6 of the Position Paper describes that a User is able to provide 'enduring consent'. Consideration must also be given to how a User can effectively withdraw consent (whether it is single-instance or enduring), and precisely what effect such withdrawal will have (eg. which data flows will no longer proceed; when the withdrawal will take effect).

The User History Log described at section 7.4.10 is a useful step towards system transparency that will engender trust. A further step that could be considered is an active notification system whereby a User might opt (in or out) to receive text messages or emails notifying them when their data has been accessed, by whom and for what purpose. The My Health Record user interface provides a useful example of such notification system design.

5. Data breach notification provisions

Section 7.4.15 of the Position Paper sets out that the existing Notifiable Data Breach scheme in the *Privacy Act 1988* (Cth) will apply and will be extended in respect of state and territory government bodies that are Accredited Participants. It would be useful to consider whether the planned lines of notification in case of a data breach could be simplified to reduce the administrative burden on those bodies who are required to notify; for instance, could OAIC share notifications with the Oversight Authority rather than a requirement that both these entities be notified by the affected body? Similarly, could the Oversight Authority share notifications with relevant state or territory privacy commissioners where the breach affects a state or territory government body not subject to the *Privacy Act?*

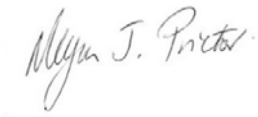
Beyond the proposed 'mechanism for information-sharing for data breaches between regulators including the OAIC', it is important that there also be a mechanism for public reporting of data breaches. This reporting should occur consistently and in a central location. This would help avoid the current situation that affects reporting pertaining to breaches of the My Health Record system, which are published separately from the OAIC reports relating to the data breach notification scheme in the *Privacy Act.* Centralised reporting can better promote sector-wide assessment and improvements in data security, which is among the commonly-stated purposes of data breach notification schemes internationally.

6. Enforcement agency access

Enforcement agencies will be able to seek access to 'information about the User's behaviour on the system' (7.4.3) and - if the design of similar legislative provisions in the *Privacy Act* is adopted - Accredited Participants will be able to provide this information to enforcement agencies without judicial oversight. (See Australian Privacy Principle 6.2(e)). To promote public trust in the Digital Identity system it would be preferable that judicial oversight be embedded in any such disclosure for enforcement-related activities, as has been done within the *My Health Records Act 2012* (Cth) s 69A in response to public concern about such disclosure.

Thank you for the opportunity to make this submission.

Yours sincerely



Dr Megan Prictor, Research Fellow, Melbourne Law School
Email megan.prictor@unimelb.edu.au, ph +613 9035 9644

Dr Mark Taylor, Associate Professor in Health Law and Regulation, Melbourne Law School

Gabby Bush, Program Manager, Centre for AI and Digital Ethics