New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

DIGITAL TRANSFORMATION AGENCY- DEPARTMENT OF GOVERNMENT SERVICES

DIGITAL IDENTITY LEGISLATION POSITION PAPER

16 July 2021

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

The NSW Council for Civil Liberties (NSWCCL) welcomes the opportunity to make a submission to the Digital Transformation Agency (DTA) in regard to the public consultation on the Digital Identity Legislation Position Paper (Position Paper).

It is noted that the purpose of this round of consultation is to seek feedback to "guide the development of proposed legislation intended to support an expanded Digital Identity system (DIS) in Australia." The focus of this submission will therefore be to comment on the enshrining in law of relevant privacy and consumer protections which should be embedded in any digital identity system. There will be little or no commentary on the technicalities of privacy and consumer safeguards which are beyond the expertise of the author.

Introduction

NSWCCL welcomes the codification of the DIS which will embed privacy safeguards in primary legislation not in a subordinate instrument.

The DIS claims to include a number of privacy features. The effect and success of which will be known once the draft legislation is introduced.[1] Such features include voluntary participation, no single identifier, express consent and Privacy Impact Assessments (PIA) for accreditation.

Despite these provisions, there are clear weaknesses. The rules, for example, will allow for the PIA to be conducted by an assessor from within the same entity as the applicant; hardly independent.

There is no stand-alone independent Digital Identity Authority though the Information Commissioner oversees compliance with the privacy safeguards in the legislation. An independent oversight authority will be formed, however does not deal with privacy safeguards, only regulatory matters such as the accreditation of entities.

The legislation will prohibit accredited participants from collecting, using and disclosing information about a user's behaviour on the system, except in specific circumstances. The purpose is to prevent profiling. Prohibited purposes will include "speculative profiling on digital identity information for an investigatory purpose".[2]

---

[1] Digital Transformation Agency, Australian Government , Digital Identity Legislation Position Paper https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/digital-identity-legislation-position-paper

[2] Speculative profiling will mean data mining for the purpose of identifying individual users for further analysis or action.

Investigatory purposes are not the same as enforcement purposes under the Privacy Act since it will not cover some fraud and security purposes directly related to keep the system secure under the legislation. It will mean any of the following purposes:

- detecting, investigating, prosecuting, or punishing:
  an offence
- a contravention of a law punishable by a pecuniary penalty.
- detecting, investigating, or addressing acts or practices detrimental to the protection of the public revenue
- detecting, investigating or remedying serious misconduct
- conducting surveillance or monitoring, or intelligence-gathering activities

However, the position paper acknowledges that this does not prevent law enforcement accessing information in relation to suspected individuals under existing powers. NSWCCL strongly opposes the use or availability of private, sensitive, digital information for law enforcement purposes or any other additional purpose without appropriate oversight through the issue by a judicial officer of a warrant.

These, and the select matters raised in the rest of this submission, exemplify the likely adverse impacts on robust privacy safeguards if the DIS and legislation "don't get it right".

The Consultation Process

The consultation process for the DIS has been "too little too late". There has been inadequate time for public consultation over what is a complex and wide-ranging project. It is currently proposed to take the legislation to Parliament in the latter part of 2021. The project has cost more than $200 million over five years and "is slowly emerging from the shadows".[3] The lack of transparency and engagement with an unaware public is breath-taking. For example, the Australian Privacy Foundation have complained, over the years of the DIS development, that their attempts to be involved in the consultation process were constantly frustrated.[4] Others who made submissions to the 2020 Consultation Paper[5] complained that "A good process would be a transparent one that opens up both the documentation, code and accreditation process to public scrutiny so people like us can find the bugs they haven't noticed."[6]

Of the 34 submissions published, in response to the Consultation Paper, most were from government departments and the technology community. There were two submissions from the privacy commissioners. "The DTA said the submissions [they] were "overwhelmingly positive" with "near uniform agreement on the immense value of the digital identity system", despite one calling for the program to be scrapped and redesigned entirely, and others raising concerns about accessibility, the use of

---

- conducting protective or custodial activities
- enforcing a law relating to the confiscation of proceeds of crime
- preparing for, or conducting, proceedings before a court or tribunal or implementing a court/tribunal order
- a purpose that relates to, or prejudices, national security within the meaning of the National Security Information (Criminal and Civil Proceedings) Act 2004 but does cover fraud or security mitigation practices required by the TDIF rules or used by Accredited Participants to meet their obligations under the TDIF rules.

This means that speculative profiling will be prohibited for the above activities, but this does not prevent law enforcement accessing information in relation to suspected individuals under existing powers.
Ibid https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/digital-identity-legislation-position-paper

[3] Sadler, D (22 June 2020) DTA digital ID hit by transparency concerns, InnovationAus https://www.innovationaus.com/dta-digital-id-hit-by-transparency-concerns/

[4] Australian Privacy Foundation Submission -The Trusted Digital Identity Framework (TDIF) Project (23 August 2016) https://privacy.org.au/Papers/DTO-TDIF-160823.pdf

[5] Digital Identity Legislation Consultation paper synthesis report and submissions https://www.digitalidentity.gov.au/have-your-say/phase-1-digital-identity-legislation

[6] Professor Vanessa Teague, op.cit. Sadler (22 June 2020)

biometrics, and a lack of public trust."[7] There were no published submissions from legal rights or privacy advocates or academics, apart from Professor Teague.

The OAIC response to the Consultation Paper stated that:
"The Australian community is highly attuned to the importance of protecting personal information. At the same time the community is reporting decreasing levels of trust in information handling by both business and government. The OAIC's Australian Community Attitudes to Privacy Survey (ACAPS) 2020 results reveal:

- 85% have a clear understanding of why they should protect their personal information
- 97% consider privacy important when choosing a digital service
- since the 2007 ACAPS, trust in companies in general is down by 13% and trust in Federal Government departments is down 14%.[8]

The intended beneficiaries of the DIS appear to be government agencies and business, rather than its citizen users who face serious risks of security breach and function creep.[9]

Centralisation of Digital Identity

Though there may be little appetite for the government to make change to the DIS, having centralised digital identifiers is problematic. The DIS is a federated digital identification system which relies on identity providers who act as central repositories for identifiers.[10] "Identity Providers will control, store and manage all user information – which is likely to include birth certificates, marriage certificates, tax returns, medical histories, and perhaps eventually biometrics and behavioural information too…. Identity Providers consolidate information in one place and risk becoming a single point of failure. This exposes users to harms associated with the possibility of stolen or compromised personal information."[11]

This aspect of the DIS should be re-evaluated and alternatives to the federated DIS, which allow individuals to control their identity, should be explored. For example, self-sovereign identity (SSI) "lets you share your identity freely, confirm it digitally, and manage it independently—without the need of an intermediary."[12]

---

[7] Sadler, D (15 February 2021) DTA's spruiking of Digital ID is unhelpful, InnovationAus https://www.innovationaus.com/dtas-spruiking-of-digital-id-is-unhelpful/

[8] OAIC, Digital Identity Legislation Consultation Paper - Submission to the Digital Transformation Agency https://www.oaic.gov.au/engage-with-us/submissions/digital-identity-legislation-consultation-paper-submission-to-the-digital-transformation-agency/

[9] APF Op. Cit

[10] Scolyer-Gray, P., Jeong, J. and Zoltavkin, Y. (28 January 2020) Australia's National Digital ID is here, but the government's not talking about it. The Conversation https://theconversation.com/australias-national-digital-id-is-here-but-the-governments-not-talking-about-it-130200

[11] ibid

[12] Hancock, A. (31 August 2020) Digital Identification Must Be Designed for Privacy and Equity, Electronic Frontier Foundation https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10

The Privacy Act 1988

The Position Paper states that the DIS will "be developed in a way that recognises the potential changes being made to broader privacy protections as a result of the review of the *Privacy Act* currently underway."

Accredited participants will be required to be covered by the *Privacy Act,* with state and territory government entities having the option of complying with a comparable state or territory privacy law.

However, the reforms to the *Privacy Act* have now stalled. The Digital Platforms Inquiry Final Report (DPI Final Report) which was released by the ACCC in June 2019 made extensive recommendations to strengthen privacy protections for individuals and improve transparency and accountability in data handling practices.[13] NSWCCL opposes the DIS reliance on the *Privacy Act* for significant privacy safeguards in the legislation, until the *Privacy Act* Review is complete.

The DIS legislation should be supported by an enforceable human rights framework such as a Bill of Rights. Australia is the only Western democracy that lacks such a framework.[14]

In 2019, the ACCC recommended that a new statutory cause of action be created to cover serious invasions of privacy with the aim to reduce the "bargaining power imbalance" between individuals and digital platforms.[15] The arguments demonstrating the need for more effective protection of privacy, and for a statutory cause of action for serious invasion of personal privacy, have been extensively and repeatedly debated over the years.[16] A number of Law Reform Commissions have concluded that a statutory cause of action for serious invasion of privacy should be legislated in Australia and advised their governments accordingly.[17]

These frameworks are particularly important when considering protections to the right to identity, often not protected by privacy legislation which may screen errors from scrutiny caused by fraud.[18]

---

[13] Australian Competition and Consumer Commission (June 2019) Digital Platforms Inquiry- Final Report https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

[14] *Williams, G*. *"The Victorian Charter of Human Rights and Responsibilities: Origins and Scope"*. (2006) 30(3) Melbourne University Law Review 880

[15] Op.cit Digital Platforms Inquiry- Final Report

[16] See also NSW Council for Civil Liberties Submission on Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy (Nov 2011) https://d3n8a8pro7vhmx.cloudfront.net/nswccl/pages/601/attachments/original/1418076925/2011_submission_serious_invasions_of_privacy.pdf?1418076925

[17] These reviews resulted in three reports: New South Wales Law Reform Commission, Report 120, Invasion of Privacy (2009); (NSWLRC Report); Victorian Law Reform Commission, Surveillance in Public Places: Final Report 18, 2010; (VLRC Report) and the ALRC Report 108 in 2008.

[18] Sullivan, C (2011) Chapter Title: Digital Identity — Consequential Individual Rights, Book Title: Digital Identity, Book Subtitle: An Emergent Legal Concept *University of Adelaide Press* https://www.jstor.org/stable/pdf/10.20851/j.ctt1sq5wqb.11.pdf?refreqid=excelsior%3A92ef7086f37a4c22a5bc3835c546c485

"Consequently, interference with an individual's right to identity, that is, the right to be regarded as a unique individual under the scheme, cannot be justified on the basis that it is, for example, an unfortunate, or indeed an inevitable, consequence of a scheme which has broader societal objectives."[19]

Voluntary Participation and Equity

It is proposed in the Position Paper that the legislation will provide individuals with the right to voluntarily create and use a digital identity, including the right to deregister and not use a digital identity, at any time. However, NSWCCL recommends that the legislation must also expressly preclude conversion of the scheme from voluntary/opt-in to opt-out or mandatory (as occurred with MyHealthRecord).[20]

Opting out of essential digital interactions is not a realistic option for most individuals. Balancing interests therefore amounts to having to agree to terms of access or risking the suffering of economic disadvantage, discrimination or social exclusion.[21]

Alternative channels to Digital Identity are encouraged in the Position Paper, to enable individuals to access services, excluding essential services (such as a welfare benefit) and monopolistic services. NSWCCL strongly recommends that a commitment to simple, accessible alternatives to accessing services, particularly essential and monopolistic services, be provided in primary legislation.

The power imbalance between users of services and providers was highlighted in the OAIC's submission to the DPI:

"[C]onsumers may be informed and understand the inherent privacy risks of providing their personal information but may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative. Further, while 'consent' is only a meaningful and effective privacy self-management tool where the individual actually has a choice and can exercise control over their personal information, studies also show that consumers rarely understand and negotiate terms of use in an online environment".[22]

Equity of access and the "principles of decentralizing one's information into their own ownership are completely related to, and contextualized by, privilege." [23] The effect on vulnerable members of the community, such as the homeless, refugees, the

---

[19] ibid

[20] APF Op.cit

[21] Lindgren, E.R. (2018) Privacy from an Economic Perspective. *The Handbook of Privacy Studies* [Amsterdam University Press] at 200

[22] Australian Government, Office of the Australian Privacy Commissioner (20 November 2019) Privacy implications of the Digital Platforms Inquiry https://www.oaic.gov.au/updates/speeches/privacy-implications-of-the-digital-platforms-inquiry/

[23] Hancock Op.cit.

indigenous population and the disabled community, of not being able to access technology, is profound.

The Northern Territory government submission to the consultation paper stated that, "Substantial work is still required to address the details and issues for the community to ensure the digital identity system that is eventually implemented will meet the needs and protect the identities of all Australians,….There are many alternative pathways and potential unintended consequences of implementing such a significant change that needs to be fully considered and addressed prior to legislation being enacted."[24]

Biometrics

The legislation will propose that biometric matching in the DIS will be limited to one-to-one matching and be consent based. It will prohibit use of biometric information to conduct searches of databases to identity people. Importantly it will require identity providers and credential service providers to delete biometric information once the purpose for which it was provided is completed.

Considering the extreme risk of a specific fraud or a security incident, biometric use needs to be carefully monitored and controlled if citizens are to accept an expanded facial verification functionality. It was only recently that National Facial Biometric Matching Capability was rejected outright by the Parliamentary Joint Committee on Intelligence and Security for lack of privacy safeguards.

"The use of biometrics at any point of authentication introduces substantial privacy and security risks. Avoiding biometrics altogether would be a substantially better approach…. The exploitation of any biometric system can be catastrophic for users. Once compromised, a user's biometric cannot be simply replaced in the manner of a password or PIN…in open networks relying on variable hardware and software on user devices, the risks are substantial and cannot be effectively managed.[25]

Privacy principles

The GDPR lists key privacy principles, which include lawfulness, fairness, transparency; purpose limitation; data minimisation; accuracy; storage limitation; data integrity and confidentiality (Article 5, GDPR). These requirements should be considered in the design of the DIS.

In terms of data minimisation, the DIS proposes that records be kept for 7 years. Having provided the information in these records, how easy is it to withdraw from the scheme, and have one's data deleted?

The OAIC made recommendations that included the requirement for periodic reviews of the legislation and the Oversight Authority' performance and operation; and, a public annual report detailing data breaches, and accuracy rates of biometric

[24] Sadler, D (15 February 2021) Op.cit.
[25] ibid Veroguard submission to DIS Consultation paper

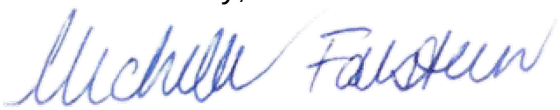
algorithms. NSWCCL supports these recommendations and a complete review of the DIS to ensure significant privacy measures are in place.

NSWCCL RECOMMENDATIONS

1. The DIS legislation should not proceed without the Privacy Act review being completed,
2. Privacy safeguards should be embedded in primary legislation not in a subordinate instrument,
3. PIA's need to be truly independent and audited,
4. A stand-alone independent Digital Identity Authority with sufficient resources and enforcement powers should be established,
5. NSWCCL strongly opposes the use or availability of private, sensitive, digital information for law enforcement purposes or any other additional purpose without appropriate oversight through the issue by a judicial officer of a warrant.
6. In the interests of transparency and accountability, the DTA must engage fully and meaningfully in consultation and education with the public and interested stakeholders,
7. Re-evaluation and alternatives to the federated DIS, which allow individuals to control their identity, should be explored,
8. The DIS legislation should be supported by an enforceable human rights framework such as a Bill of Rights and a new statutory cause of action should be created to cover serious invasions of privacy and on identity,
9. The legislation must expressly preclude conversion of the scheme from voluntary/opt-in to opt-out or mandatory,
10. A commitment to simple, accessible alternatives to accessing services, particularly essential and monopolistic services, should be provided in primary legislation to protect vulnerable citizens,
11. Biometric use, if it cannot be avoided completely, needs to be carefully monitored and controlled. Substantial work needs to be done in this area by the DTA to ensure a significant standard of protections are afforded the Australian people, especially considering the growing call for a moratorium on the use of biometric software,
12. The key privacy principles, of lawfulness, fairness, transparency; purpose limitation; data minimisation; accuracy; storage limitation; data integrity and confidentiality should be embedded in the DIS and integrated into the legislation,
13. Periodic reviews of the legislation and the Oversight Authority' performance and operation; and, a public annual report detailing data breaches, and accuracy rates of biometric algorithms and
14. The promised privacy safeguards should be included and strengthened.

This submission was prepared by Michelle Falstein on behalf of the New South Wales Council for Civil Liberties.

Yours sincerely,



Michelle Falstein
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission- Michelle Falstein:
email michelle.falstein@nswccl.org.au;
Tel 0412980540