14 July 2021

Inputs to Australian Digital Identity Legislation Position Paper (Phase II consultation by the Digital Transformation Agency)

We thank the Australian Digital Transformation Agency (DTA) for holding this additional round of consultation on its Digital Identity programme, including the new Digital Identity Legislation Position Paper (the Position Paper).

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT, and are a member of the global Forum of Incident Response and Security Teams (FiRST). We have special consultative status at the United Nations[1] and we also facilitate the **#WhyID** community - a community of more than 200 organisations and experts from across the world working towards ensuring that digital identity programmes respect the rights of users.[2] This community has also led an open letter in 2019 to international organisations and governments, expressing their concerns and asking some primary questions which help in ensuring that digital identity programmes are designed and implemented to ensure the protection of user rights.[3] This letter highlights the basic human rights concerns that arise from many national and humanitarian digital identity programmes, and raises questions that stakeholders must address to ensure that digital identity programmes protect human rights. We write to you to provide our initial comments based on our expertise working on different digital identity programmes across the world.

---

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] Access Now, #WhyID, https://www.accessnow.org/whyid/
[3] Available at https://www.accessnow.org/whyid/ [A copy of the fully #WhyID international letter has also been filed as a supplemental input to this consultation]

As we noted previously in our comments towards the initial consultation organised by the DTA, the experience across many nations recently has shown that digital identity systems can soon pervade the lives of individuals, become gateways for important services, and in many instances become the foundation for a person's legitimacy or citizenship in a country or region. They have very real impacts on people's daily lives, particularly for those less privileged. It is clear that digital identity systems impact human rights.

In our earlier submission, our overall comments had focused on the following key pillars regarding our policy approach and guidance:

- At this initial stage, we are cautiously optimistic about the approach currently proposed by the DTA for a national approach towards digital identity in Australia. **A federated architecture, purpose-centric digital system to enable the recognition, authentication, and use of multiple provider identities** is the manner to approach a digital identity system if one was seeking to advance such a system in a jurisdiction. An ideal policy approach **should not restrain multiplicity of digital identity**. For digital identity to be empowering in a given context, the technological, legal, and policy framework must be built on a foundation of user agency and choice, informed consent, the space for anonymity, and respect for privacy. A framework enabling multiple identities, which are tailored to a specific purpose and limited by data collection requirements, would enable innovative solutions which protect rights of users. individuals must be given a choice in digital identity architectures through multiplicity and purpose limitation.
- We **advise against an approach that favours biometrics as the primary authentication channel at most times in a digital identity system**. Requiring individuals to put their personal, unchangeable, biometric and sensitive data at great risk of privacy intrusions should be a measure of last resort for the purposes of "proving" legal identity. We also believe that public authorities should seek to avoid the usage of facial recognition technologies embedded in centrally-run systems as far as possible, and would caution against such use in this programme in Australia.
- Any scheme design on digital identity depends on **an effective legal and governance framework for both data protection generally as well as further, supplementary restrictions and oversight on digital identity specifically**. **The mere existence of a data protection framework is not enough**; there needs to be an effective data protection framework and regulator that can regulate public and private sector participants in the digital identity ecosystem in coordination with additional specialised governance or regulatory bodies. The digital identity system must be set in place by specific legislation passed by Parliament, with as much of its subordinate rules subject to legislative oversight and properly balanced with the existing privacy and data protection framework.

Building on our initial, key recommendations made in our previous filing and summarised above, we provide below additional specific comments based on the current Position Paper. We look forward to seeing the draft legislation as the DTA and the Australian Government as a whole go into the next stage of this consultative process; our current comments here are brief and will be expanded upon as we see the draft legislative text and as further information is made available for consultation. We are providing inputs on a chapter-wise basis for key portions of the present position paper:

Structure of the Digital Identity Legislation

- *On Ministerial rulemaking powers, codification into primary legislation, and parliamentary oversight:*

We appreciate the efforts made by the DTA to respond to the concerns raised by many stakeholders regarding the proposed amount of delegated legislation and rulemaking that was described in the first consultation paper. The current Position Paper does well to recognise that several areas of rulemaking require not only clear notice and comment periods, but should also be subject to parliamentary control via the "disallowable instruments" route. The Position Paper also provides some clarity by including a diagram (page 12) that illustrates the pyramidal structure of disallowable instruments, notifiable instruments, and administrative guidelines functioning under the Trusted Digital Identity Bill. However, improvements can still be made.

As we note later in this submission, several of the privacy related measures would still be better placed to be directly included in the primary legislation, rather than rulemaking. We draw attention to the explicit warning and guidance provided by the Office of the Australian Information Commissioner (OAIC) in this regard in their comments to the December 2020 consultation, where they said:

> "Embedding privacy protections in primary legislation also guards against inadvertent or unforeseen risks to privacy, such as the collection, use or disclosure of personal information that may not have been originally intended, known as 'function creep', or that which may not be reasonable, necessary and proportionate to the relevant policy objectives."[4]

Given the complicated range of proposed rulemaking and administrative guideline powers, the DTA should make available as part of this current consultation a table outlining the different proposed issues for rulemaking and the type of instrument they are proposed to be.

[4] https://www.oaic.gov.au/engage-with-us/submissions/digital-identity-legislation-consultation-paper-submission-to-the-digital-transformation-agency/

Scope of the Digital Identity Legislation

- *Extent of the Digital Identity Legislation:*

We believe that the scope of the legislation can include digital identity systems operating in Australia beyond just the current system. Creating a baseline legal framework that can enable specialised guidance in this area along with the general requirements of the Privacy Act would help provide more certainty and reduce the need for further legislation in the future. It would be ideal at minimum to have one overall digital identity law applicable to public sector digital identities and digital identity systems in Australia, including more coordinated oversight, rights and remedies for individuals.

- *Defining the Digital Identity system:*

The Position Paper indicates that the aim of providing certainty as to how the Digital Identity System will operate will be enabled by the Minister making a rule describing the system and referencing the identity exchange managed by Services Australia within that definition. Given the importance of clear legislative control on the scope of the system, it would be better that this description of the system is included in a disallowable instrument subject to parliamentary review - if not in the primary legislation itself.

- *On the legislative framework overseeing the use of facial recognition in the digital identity system:*

In our previous submission, we had stated that "the relationship between the proposed legislation on Digital Identity and the Identity-matching Services Bill needs to be more carefully explained and spelt out, to prevent inconsistency or clashing provisions between these two proposed laws". Regrettably, we believe that this has still not been fully addressed in the present Position Paper. The most recent text makes it clear that the proposed digital identity system will include at least some use of one-is-to-one facial recognition in the form of the Face Verification Service (FVS). It then specifically notes that the FVS will be used as a verification tool by identity providers, while not providing any clarity on the legislative framework to oversee that. Specifically, it is stated in the Position Paper that:

> "There has been no change to the position that the Document Verification Service (DVS) and Face Verification Service (FVS) will not be covered by the Legislation. These services are verification tools for identity providers and are expected to be subject to their own standards and legislation. The Legislation is not intended to replace the FVS or DVS as these services are key inputs for identity providers to verify attributes of a User creating a Digital Identity."

Previous documents as part of the DTA's Digital Identity consultations had indicated that the FVS and DVS were expected to be covered by the Identity-matching Services Bill 2019. However, given the

pause and reconsideration of that proposed legislation given the significant concerns raised by the Parliamentary Joint Committee on Intelligence and Security, it is presently not clear what - if any - legislative framework will be promulgated to better oversee such systems, the facial recognition processes they leverage, and to which agencies such systems are made available. We believe that the Trusted Digital Identity Bill must provide oversight in this area - even if transitional - given how they comprise key parts of the identity ecosystem in Australia.

Governance of the Digital Identity system

- *Appreciate the Position Paper providing further details regarding establishment and independence of the Oversight Body:*

The Position Paper has responded to earlier stakeholder comments seeking more clarity on how the Oversight Body would be established, and what measures would be taken to ensure its independence. We believe that the Bill should further indicate how the Oversight Body would be accountable to parliament as well as open to stakeholders in the wider identity and privacy ecosystems, and also include further safeguards in the appointment process in order to ensure the independence and public trust of this critical new office.

- *Role of Information Commissioner as being responsible for privacy functions:*

The Position Paper has done well to make the proposed role of the OAIC much clearer within the outlined scheme. Given the significant advisory, oversight, regulatory, and reporting roles being placed on it by the proposed Bill, it is crucial that it also outline the resourcing implications for the OAIC and provide for adequate support accordingly.

- *Automated decision-making use may require additional safeguards:*

If the Digital Identity System and accompanying Legislation propose to allow for certain decisions to be made by use of automated process, there must also be accompanying provisions providing individuals a right to be able to seek an explanation for such decisions and related avenues for challenge and redress. This may be placed within the Oversight Body, along with a reporting obligation around the use of such automated processes being documented and aggregate information regularly published.

Privacy and consumer safeguards

- *Concerns around the retention period, and proposal to have Digital Identity Bill have overriding effect on Privacy Act with respect to record keeping:*

The Position Paper outlines a significantly long retention period for metadata and activity logs- up to seven years or another period to be specific by the Minister in the rules. This can cause potential privacy and digital security harms to individuals and participants in the system. The Position Paper also specifically proposed that the record-keeping requirements in the Bill will override the Privacy Act if there is any inconsistency. We do not believe that a provision overriding the Privacy Act here is justified, and we urge for the proposal to be dispensed with.

- *Prohibition on exchanges retaining attributes should be included in legislation, and not just rules:*

The Position Paper is good in its emphasis on prohibiting identity exchanges from retaining attributes as part of identity related transactions. However, this prohibition is currently only proposed to be enabled via rulemaking by the Minister subsequently. Given that this is a critical principle key to ensuring a healthy, privacy respecting digital identity ecosystem, we believe it is crucial to include it in the primary legislation itself.

- *Further, statutory restrictions regarding biometrics must be included in the primary legislation:*

Although we advise against the use of biometric authentication until certain requirements can be proven, we believe that the proposed Bill must contain specific provisions governing the use of biometrics. These must not only be done by rulemaking subsequently and subject to the discretion and changing desires of the executive branch. Specifically in this regard, we support the earlier recommendations made by the OAIC to the DTA in its submissions to the previous stage in the digital identity consultation:

> "The Paper proposes that the safeguards around the use of biometric information include:
>
> - an oversight regime for the use of biometric information
> - limiting the use of biometric information to permitted purposes
> - prohibiting the disclosure of biometric information to certain third parties, and for certain uses
> - consent and deletion requirements for the use of biometric information.
>
> The OAIC supports the DTA's proposal to complement protections set out in the Privacy Act by installing these additional safeguards. As noted above the OAIC recommends that these

> safeguards remain in the primary legislation and suggests that the legislation exhaustively prescribe which types of biometrics are permissible for use in the system…
>
> … transparency mechanisms such as the publishing of an annual report detailing data breaches, PIAs and accuracy rates of biometric algorithms, among other things, to assure individuals that there is adequate oversight of how their personal information is being handled."

The Trusted Digital Identity Bill must contain specific provisions in the primary legislation that seek to impose safeguards on the use of biometrics information pursuing a safe, inclusive system that is not liable to errors, advancing the international legal standard of necessity and proportionality. This must be coupled with oversight mechanisms and remedy for users, and allowing other methods of authentication. In addition to this, there must be statutory reporting requirements around the use of biometric information, particularly around the accuracy rates of biometric algorithms being used by actors within this ecosystem.

- *Exceptions to the mandate to provide an alternative channel for identity should be further tightened:*

In our earlier submission we noted:

> "Voluntary" should extend to the choice of digital as a whole and not just be about a choice between different services providers. We believe that the rationale given to exclude certain entities from a requirement of providing alternate verification processes is a slippery slope, most notable the proposition that "*requiring certain relying parties such as local councils, small government agencies or the private sector to provide an alternative channel will not be practical*".

Our policy position is that digital IDs can serve as a form of exclusion, particularly when there is a lack of a meaningful alternative. To this end, we reiterate our recommendation that all digital identity systems are voluntary.

We regret that the Position Paper [specifically, para 7.4.1] exempts relying parties from the requirement of providing an alternative channel for digital identity, for "essential services," which includes welfare benefits, or for "monopolistic services". We recommend that this be altered, noting that it is often persons who are reliant on the welfare system who are most in need of a choice, and most harmed by the lack of a choice. We also advise against broad grounds such as "commercial" or "practical feasibility," on which relying parties can apply for exemptions to provide alternative channels.

- *On interaction with the overall surveillance regime*

In our submission in December 2020, we noted the following requirements regarding access to data and surveillance in the context of digital identity programmes:

> *Access of data maintained by any national digital identity programme by law enforcement or other state actors must be governed by relevant international legal standards, particularly the "Necessary and Proportionate" principles,[5] in the absence of stronger domestic safeguards set out by law. Biometric data as well as other key types of sensitive data, such as information for authentication or identification requests to the system, should be recognised as "protected information". Relevant legal frameworks or regulations should institute access accountability measures, by, for instance, mandating that the issuer of the national digital identity must maintain an access log that is associated with the identity for the user to consult at any time. The access log should contain the following information: who accessed the data, when, where, and for what purpose.*

Overall, the framework envisioned does not address how this interacts with the wide powers of access to data and the compelling of digital information to law enforcement and security services currently made possible by different Australian statutes.

We note that Section 7.4.3 of the position paper lays out restrictions on the use of data for profiling. However, Accredited Participants can collect, use, and disclose information about a user's behaviour on the system for a "lawfully made request for enforcement purposes" (as defined in the Privacy Act).

Without adequate safeguards, wide access to user data could undercut the intended safeguards against the creation of an all-encompassing government profile. We recommend that the Trusted Digital Identity Bill contain specific guidelines on how these requests are made, in order to have sufficient safeguards against scope creep; and reiterate our recommendation that access to data by law enforcement or other state actors must adhere to the Necessary and Proportionality Principles.

Administration of charges for the Digital Identity system

In our earlier submission we warned against service fees for public services, noting that:

> At a broader level, adding service fees to the provision of digital identity programmes can lead to predatory outcomes for users. Many digital identity programmes are used as a means of delivering essential services. Adding service fees in this context would effectively mean charging citizens for free services they are entitled to. Further, mixing financial incentives with service delivery can cause problems, and digital identity programmes

[5] Necessary and Proportionate Principles, https://necessaryandproportionate.org/principles.

established or administered by governments should not be set up as profit-making entities but rather as public goods. We therefore generally caution that service fees should not be added to public sector digital identity programmes.

We appreciate the charging framework outlined in Section 11.4; but note that this still envisages a situation where costs are "passed on" to users.

CONCLUSION

Thank you for the opportunity to participate in these consultations. We remain available for any clarification or queries in relation to this feedback, and hope to be of further assistance in this important process.

Yours sincerely,

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
Access Now
raman@accessnow.org

This submission was prepared with the assistance of Ria Singh Sawhney and Namrata Maheshwari with the Access Now Asia Pacific policy team, and prior inputs from Naman M. Aggarwal.