27 October 2021

Inputs to Australian Trusted Digital Identity Bill Exposure Draft (Phase III 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 Australian Trusted Digital Identity Bill Exposure Draft (the Exposure Draft).

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 continuing inputs 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/

As we have spoken to in our publication earlier this month on 'Busting the dangerous myths of Big ID programs', the quickly expanding "Big ID" industry around the world has driven the adoption of centralized digital identity programs that severely undermine human rights.[4] Governments, companies, and international agencies sell and buy the idea of implementing a Big ID project as the silver bullet for solving a host of problems: more efficient delivery of public services, closing gaps in identification, fraud prevention, crime detection, and more. But far too often, these systems overpromise and underdeliver, without ever presenting evidence that these tools will actually be effective at meeting people's needs, and put millions of people's rights at risk in the process. We therefore caution all policymakers to learn from the lessons of recent Big ID programmes and be aware of the myths that Big ID champions often propagate.[5]

We have previously provided our comments on the direction and approach of the Digital Transformation Agency in its Trusted Digital Identity Framework in the two earlier phases of consultation organised by it. In this submission, we are providing our initial comments on the current exposure draft version of the Trusted Digital Identity Bill 2021 made available by the DTA earlier this month. Given the detailed nature of the exposure draft version of the proposed bill and its accompanying other documents, we respectfully submit that a more extended consultation period in this round of stakeholder engagement would have been more beneficial. Providing less than one month for stakeholders to study the exposure draft and its related documents will result in a less effective consultation with reduced participation. We therefore request the DTA for additional opportunities for input from civil society, technical experts, and public interest representatives over the following month.

As we have mentioned previously, we have been cautiously optimistic at the careful, considered, and incremental approach taken by the DTA in its Digital Identity consultations. The exposure draft currently demonstrates that some of the concerns that we and other stakeholders have flagged previously have been recognised by the DTA, with attempts made to address them in the present language of the proposed bill. However, we believe that the DTA and the Australian Government as a whole must remain cautious around further deployment and proliferation of inter-connected digital identity systems. While federated architecture and a purpose-centric digital system to enable the recognition, authentication, and use of multiple provider identities is a promising way to approach a digital identity system, **an ideal policy approach should not restrain multiplicity of digital identity, or privilege online modes of access to government services**. The Australian model has a long way to go in ensuring that it does not result in the creation of a surveillance architecture and that peoples' rights are placed at the center of any new programme. The Australian government must ensure that the purpose of the Digital ID system is clearly articulated and placed at the center of any programme.

[4] Access Now, *Big ID, bad idea: busting ID myths that are endangering human rights*, 5 October 2021, https://www.accessnow.org/big-id-endangering-human-rights/.
[5] Access Now, *Busting Big ID's myths*, 5 October 2021, https://www.accessnow.org/busting-big-ids-myths/.

Additionally, we continue to remain concerned regarding the emphasis on more widespread use of biometrics being advanced by the DTA, including in the present exposure draft. **Biometrics should not be favoured as the primary authentication channel in a digital identity system.** As we have consistently indicated in our submissions across the different consultative phases organised by the DTA, the Australian digital identity framework should consider technical alternatives to permit the verification of identities which should be considered, including chip-based authentication or encryption-enabled key-based models.

We also correspondingly **caution against solely relying on a legislative framework to combat the harms that can be caused by a digital identity system**; the Australian Government must also continue to consider the overall approach and architecture proposed for the system and whether alternative approaches can help advance policy interests in a manner more respectful to human rights. We agree with the concerns raised by researchers Ben Fringley and Vanessa Teague in their earlier submission to the DTA noting that "Legislating to make it secure by at will not stop organised crime, foreign governments, or ordinary criminals, from taking advantages of its design flaws", and that **further study and consideration should be made of digital identity frameworks that rely on public key infrastructure**.[6] At the very least, we believe that any Trusted Digital Identity Bill and the oversight architecture it creates should allow for the use of public key infrastructure based approaches to digital identity in Australia.

We provide further initial comments and recommendations below, addressing specific areas within the present exposure draft version of the proposed Trusted Digital Identity Bill:

■ Privacy chapter in exposure draft

We welcome the attempt to create a comprehensive set of provisions exclusively on privacy and data concerns relating to the digital identity system in the proposed bill. In particular, we appreciate the following provisions and believe they are crucial to include in the final version of this proposed law:

- Requiring express consent for disclosure of attributed of individuals to relying parties and regulating disclosure of restricted attributed of individuals (sections 73, 74)
- An explicit prohibition on "single identifiers" in the digital identity ecosystem (section 75)
- The explicit prohibition on data profiling (section 80);
- The restrictions placed on digital identity information being used for prohibited marketing purposes (section 82);

[6] Ben Frengley & Vanessa Teague, *Submission to the Consultation on Digital ID*, December 17 2020, https://www.digitalidentity.gov.au/sites/default/files/2021-01/consultation01-vanessa-teague.pdf

We also appreciate the effort being made to explicitly outline the interaction of this proposed bill's privacy provisions with the Privacy Act 1988, including a clearer relationship with the Office of the Information Commissioner. However, this approach is contingent on the final form of the Privacy Act itself, which is currently undergoing review. If the Trusted Digital Identity Bill is made into law prior to changes being made to the Privacy Act as part of the in-progress review of the latter, it would likely result in legal inconsistency and potentially clashing language, oversight mechanisms. **We therefore strongly recommend that the Trusted Digital Identity Bill should only be enacted into law after the Privacy Act review process - and any corresponding amendments - have been completed**.

In addition, it is heartening to see the recognition and explicit emphasis made by the DTA in the present exposure draft and its consultation of the concerns that stakeholders have expressed regarding law enforcement and intelligence agency access to the digital identity ecosystem. The explicit prohibitions on law enforcement access to biometrics and restrictions on access to digital identity information is a useful baseline standard. We however do recommend that they be strengthened, with **clearer standards placed on law enforcement or other government agency access to digital identity information, along with additional provisions on the disclosure and public reporting of such activities, as well as mechanisms for impacted individuals to seek remedy and redress if such powers, exceptions have been unlawfully used**. This could take the form of specific powers and reporting requirements granted to the Information Commissioner, or other legal architecture for remedy and redress for impacted individuals.

We are concerned that the privacy chapter currently lacks specific provisions on the following, and recommend that corresponding sections or additions to existing sections be made:

- Adding an explicit right for individuals to seek the deletion of their data, including digital identity information besides biometrics. The present language in sections 61 and 79 are insufficient;
- Including specific provisions regulating the use of facial recognition, including the specific use of face matching, and providing a mechanism for individuals to seek remedy and redress from a public authority if they are impacted by abuse in this area. 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.

■ Oversight Authority requires further independence from executive branch

We welcome the initial efforts being made in the exposure draft to create a dedicated Oversight Body to focus on the digital identity focused sections in the law and oversight in that regard, as a complimentary measure to the role of the Information Commissioner on privacy focused provisions. However, the current language of the exposure draft that would allow the Minister to have full authority to create and appoint the Oversight Authority by legislative instrument undermines the independence of this critical institution. Given that government agencies will play a critical role in this ecosystem - acting as providers as well as other ecosystem entities - it is even more crucial that the Oversight Authority is even more explicitly set up as an independent oversight and regulatory institution, with sufficient buffer space from the executive. We therefore strongly recommended that the creation of the Oversight Authority should be specific in the parent statute itself and not fully delegated to the Minister to exercise via legislative instrument. Furthermore, it is important that the statute itself outlines the appointment process and ensures that there is independent, multi-stakeholder input into the appointment process for the individuals being chosen to head the Oversight Authority.

■ Further strengthening individual-choice in the digital identity ecosystem

We welcome the recognition by the DTA in the present exposure draft of our previously stated concern around allowing a wide definition of “essential services” for the purpose of exempting relying parties from providing an alternate channel for digital identity. In particular, **we welcome the present language in section 30 around specifically ensuring that the generation and use of digital identity is voluntary**, and that the Oversight Authority must not grant an exemption from providing an alternate channel if the requesting entity provides an essential service, or is a sole provider of services, or otherwise impacts the public interest. It is also crucial to further consult with stakeholders on what the Oversight Authority would need to do in practice in order to enforce and implement this section, including the Oversight Authority’s accessibility to vulnerable communities and less privileged individuals.

We do believe that **a specific provision needs to be added regarding the rights of individuals in the digital identity ecosystem regarding the use of automated processes**. If the Digital Identity System allows for certain decisions to be made by use of automated processes, there must also be an accompanying provision added 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.

CONCLUSION

Thank you for the opportunity to participate in these consultations. We remain available for any clarification or queries in relation to these initial comments on the exposure draft, 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