18 December 2020

Inputs to Australian Digital Transformation Agency consultation on proposed Digital Identity legislation

We thank the Australian Digital Transformation Agency for the opportunity to provide comments to this important consultation. 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 also have special consultative status at the United Nations.[1] We write to you to provide our initial comments based on our expertise working on different digital identity programmes across the world.

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**.

At Access Now, we promote rights-respecting approaches to the design and implementation of digital identity systems. Our paper *National Digital Identity Programmes: What's next?*[2] provides 15 principles — covering data protection and privacy, governance, and cybersecurity — that serve as benchmarks for ensuring digital identity systems protect human rights along with an appended short set of policy recommendations regarding the use of biometrics in digital identity programmes. We provide more specific recommendations relevant to the specific questions posed by the consultation later in this

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] Access Now (May 2018). National Digital Identity Programmes: What's next? https://www.accessnow.org/accessnow-digital-id-paper [A copy of our full report has also been filed as a supplemental input to this consultation]

submission, but believe it is useful at the outset to note the top level recommendations from our earlier report:

1. GOVERNANCE

1) Undertake transparent, inclusive and open consultations at the initiation of any digital ID programme proposal
2) Ensure a defined and restricted scope of use for the digital ID programme, provided for in the law;
3) Make enrollment and use of the digital ID voluntary;
4) Create independent and well-designed mechanisms for grievance and redress; and
5) Ensure inclusion at the enrollment stage, and no exclusion during implementation, due to technology or infrastructural capacity gaps.

2. DATA PROTECTION AND PRIVACY

1) Limit the purpose for which these data are collected and used. Put in place proper measures to prevent user profiling based on the data volunteered;
2) Grant individuals rights related to their own data, such as accuracy, recitication, and opt-out;
3) Institute robust data protection frameworks to which digital ID programmes are subject;
4) Minimise the amount of and type of data governments and associated service providers collect; and
5) Restrict lawful interception and monitoring of digital ID use and implement measures for accountability.

3. CYBERSECURITY

1) Institute capable and secure foundational technology infrastructure;
2) Ensure that data collection and storage are not centralised;
3) Separate the functions of identification and authentication and avoid creating centralised transaction logs for authentication;
4) Institute "privacy by design" principles in the programme;
5) Ensure that national ID programmes are based on models for secure communications, including providing end-to-end encrypted traffic as far as possible.
6) Provide transparency in terms of disclosure of cybersecurity policies;
7) Provide a legal and policy framework that incentivises reporting and disclosure of vulnerabilities; and
8) Take steps to notify affected parties in case of breach of data.

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.[3] This community has also led an open letter last year 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.[4] 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.

Being clear about the intent and justification for a digital identity programme is a critical step, and we are heartened to see the background and detailed explanations provided by the DTA in this consultation paper to explain why this programme is being advanced in this matter at the present point of time. We believe that this partly addresses some of the suggestions put across in the WhyID open letter, but recommend again that the DTA and Australian policy-makers pay heed to the specific questions:

#WhyID

- **Why** do we need these foundational digital identity systems? What are their benefits?
- **Why** are such programmes deployed without sufficient evidence of the benefits that they should deliver? How do these programmes plan to reduce the risk to and safeguard the rights and data of users?
- **Why** should it be mandatory – either explicitly or de facto – for users to enroll onto these programmes? These programmes are either mandatory through legislative mandates or through making them a precondition to essential services for users.
- **Why** are these programmes centralised and ubiquitous? Why is one digital identity linked to multiple facets of a citizen’s life?
- **Why** are countries leapfrogging to digital identity programmes, especially in regions where conventional identity programmes have not worked? The scalability of digital identity programmes also makes their harms scalable.
- **Why** are these digital identity programmes not following the security guidance coming out of various expert academic and technical standard-setting bodies on the use of biometrics in identity systems?
- **Why** are some private sector enterprises being privileged with access and ability to access the ID systems and build their private businesses on top of them? What safeguards are being implemented to prevent the misuse of information by the private sector? What should be the role of the private sector in the identity ecosystem?”

[3] Access Now, #WhyID, https://www.accessnow.org/whyid/

[4] 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]

At this initial, overview 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.

Some government and public authorities are tempted by the approach of a centralised, directly administered national identity system, which precludes the use of multiple forms of identity. We believe it is not essential that one single identity be used for all purposes between a person's life and death. Single-solution identity systems can prove coercive for users and act as a precondition for accessing services.

Further, due to their ubiquity, these identity systems can enable surveillance and profiling schemes by governments and privileged private-sector actors. These digital identity systems often feed databases that connect multiple aspects of a person's life, heightening the risk of profiling. These risks are accentuated if the legislative scheme for privacy and institutional frameworks for protecting human rights are in stages of development or major change.

Mandatory enrollment requirements around a single digital identity programme further exacerbate the risk of exclusion, profiling, and surveillance. This is the case whether the enrollment requirements are explicit (e.g. when a government makes possession of a particular form of national digital ID mandatory by a specific law or edict) or coerced (e.g. when the national digital ID is required to access services from other public agencies, or when governments pressure private companies and platforms to adopt mandatory use of such IDs).

A well designed and rights respecting approach to digital identity **requires care around any proposed use of biometrics**. In our previous guidance around the specific use of biometrics in our wider policy paper on national identity programmes, we recommended the following:

1. Avoid creation of centralised databases of individuals' biometric data	**2. Ensure that providing biometric identifiers is voluntary and opt-in, not a default (security) measure.**	**3. Minimise data collection and transfers.**
4. Make certain that devices that scan the user's biometric data are tamper proof and never store the actual biometric data	**5. Develop legal procedures and evidentiary standards for biometrics with care to protect human rights and due process.**	

It is heartening to see that the model proposed by the DTA in the present digital identity consultation appears to respect many of our concerns. That includes limiting biometric authentication to one-to-one authentication transactions and requiring biometric information to be deleted by accredited participants after it has been used for the purpose for which it was provided - though this is subject to the exceptions discussed in section 4.5.2. Avoiding centralised biometric data storage and favouring user device based biometric authentication is the approach that is better and more appropriate for policymakers to follow when considering the use of biometrics in a user-choice driven approach to digital identity.

We would still **caution against an approach that favours biometrics as the primary authentication channel at most times in a digital identity system**, and our comments to the specific questions on that point further help explain that. 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. Legal identity can be verified in a variety of different ways, such as chip-based authentication or encryption-enabled key-based models. The risks to individuals are accentuated in communities where people have less reason to trust public authorities, including rural communities and those of marginalised people, such as refugees or other minority groups, or communities where structures and laws are not strong enough to safeguard the individuals' rights. 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.

The collection of large amounts of personal information pertaining to identities — including biometrics — often form tempting targets for criminals and other actors for malicious hacking and cyber intrusion. Highly critical personal information is carried through programme networks. Thus, properly protecting system communications, such as requests and responses for authentication, is essential for ensuring security. End-to-end encrypted communications throughout any digital identity system is of crucial importance to ensuring digital security and must be established to the greatest extent possible.

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**. **<u>The mere existence of a data protection framework is not enough</u>**; 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. It is essential that data protection frameworks provide a well-functioning law and regulator. The law should be accountable to citizens, and institutions responsible for the law's enforcement should be independent and capable of overseeing and regulating it. Additionally, given its critical importance, regulations should go further in the context of national digital identity systems to meet at least the minimum requirements of a globally compliant data protection law and provide identity-specific rights. 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.

Further, in many countries the state is the largest collector of data and in charge of the digital identity programme, making surveillance reforms just as essential as data protection laws in ensuring users' rights. Access to data and information must be governed by rule of law, backed by narrow and specific legislation, and guided by the principles of necessity and proportionality. Given the role of the state in maintaining the data in a digital identity system, safeguards must be put in place to ensure that intra-government access to data does not happen without specific mandate. The role of judicial and quasi-judicial offices in obtaining such mandates should be explored and instituted.

In the following section of the submission, we provide more specific answers to the key questions from the consultation paper that we see relevant to our guidance and expertise on digital identity, human rights, and user-centric approaches to privacy and cybersecurity.

Responses to the questions listed in the November 2020 consultation paper

Question 1A Are the matters (legal authority, privacy protections, governance, amendments) relevant matters which should be included in the Legislation?

1. **Yes**
2. No

Question 1B Are there additional matters which should be considered?

1. **Yes**
2. No

Question 2A What matters covered by the TDIF should be incorporated into the primary legislation?

1. **security**
2. **privacy**
3. **accessibility**
4. **usability**
5. service operations
6. fraud prevention measures
7. technical integration matters
8. other (please specify)

Question 2B What matters covered by the TDIF should be incorporated into Operating Rules?

1. security
2. privacy
3. accessibility
4. usability
5. **service operations**
6. **fraud prevention measures**
7. technical integration matters
8. other (please specify)

Question 2C What matters covered by the TDIF should remain as policy?

1. security
2. privacy
3. accessibility

4. usability
5. service operations
6. fraud prevention measures
7. **<u>technical integration matters</u>**
8. other (please specify)

Explanation for the above choices: Issues relating the privacy, security of the system, and requirements regarding accessibility and usability are core to the functioning of the digital identity system and impact individual users the most significantly. These elements should be set in place in the legislation itself as core principles for the programme, its governance, and setting in place the rights and remedies available to stakeholders. Elements such as service operations and fraud prevention are important but may change, and would be better placed as operating rules which can be updated by the oversight body or supervised executive. Technical integration would require frequent revision and updation, and would be better suited to remain a policy document.

The consultation paper suggests that the obligations on relying parties in the system should be covered by the operating rules. We believe that ensuring that this element is carefully governed is an important matter to address - one that is important enough that at least principles regarding the same should be contained in the primary legislation.

Similarly, the important issue of the rules around enforcement powers of the Oversight Body for non-compliance by participants in the system should also be at least partly contained in the primary legislation, and not solely in the operating rules.

Question 3 Is a publicly available ‘Digital Identity Participant Register’ an appropriate mechanism to communicate who will be covered by the Legislation?

1. **<u>Yes</u>**
2. No

Additional comment: It is concerning that the legislation would not apply to the Document Verification Service or Face Verification Service. The paper notes elsewhere the fact that proposed statutory measures regarding them are contained in the Identity-matching Services Bill. However, 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.

Question 4 Are the proposed obligations on relying parties described reasonable?

1. **Yes**
2. No

Question 4 [second part] Should there be any additional obligations in addition to the proposed obligations on relying parties?

1. **Yes**
2. No

Question 5 Are the concepts outlined appropriate to include in a definition of ‘Digital Identity’ for the Legislation?

1. **Yes**
2. No

Comment: In particular, we commend the consultation paper clarifying that a digital identity “will correspond to only one person, but a person can have multiple Digital Identities with different identity providers”. This recognises the importance of a competitive digital identity ecosystem and avoiding a force-fitted singular digital identity model that we cautioned in the initial section of this submission.

Question 6 Does the legislation need to include a definition of Digital Identity information, or is it preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts?

Comment: We believe that the legislation should define what digital identity means for its purposes and the system overall, noting that the definitions of persona, sensitive, or protected information are those contained in previous Commonwealth Acts.

Question 7 What factors should be considered in the development of a charging framework for the system?

Comment: The current proposal on the charging framework leaves significant details for a future proposed document and consultation. At this point of time, the lack of details makes it difficult to provide specific suggestions on this. We submit at a broader level that 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 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, but may have additional inputs if the DTA provides more clarity and information around the proposed charging framework.

Question 8A What factors should be considered in the development of the liability framework?

Question 8B In what circumstances should Participants be held liable under the liability framework?

Question 8C What remedies and/or redress should be available to aggrieved Participants and Users for loss or damage suffered as a result of their use of the system?

Question 8D What other best practice mechanisms and processes should be considered to support Users when things go wrong?

Comment: Governments, vendors, and standard setters must also take responsibility for the impact and accuracy of their systems. Rights and remedies must be provided to individuals to maintain accountability of governments, vendors, and standard setters. Under the UN Guiding Principles on Business and Human Rights, companies have a duty to “know and show” their respect for human rights through due diligence, developing policies to prevent adverse impacts, and remedial measures to account for harm they’ve caused or contributed to. Transparency is a prerequisite for such accountability. Vendors, suppliers, and standard-setting organisations must bear the responsibility for the potential impacts of their technology and policies, and work with stakeholders to prevent and mitigate any salient risks.

Individuals should have appropriate mechanisms to seek redress for grievances related to abuse or misuse of their personal data as well as for data breaches. To that end, public authorities should keep detailed logs when officers access retained data, and document and retain records detailing the purpose of such access

Additionally, we commend the current approach outlined in the consultation paper that explicitly states that the remedies available to users under the liability framework would only supplement and not replace remedies available to users under other laws, including the Privacy Act.

Question 9A Should the proposed privacy and consumer protections listed be enshrined in primary legislation?

1. **Yes**
2. No

Question 9B Are additional protections required? If so, what?

1. **Yes**
2. No

Question 10A Should the Legislation include rules around the extent of choice available to Users to verify their identity?

1. **Yes**
2. No

Question 10B Should any types, or all types of relying parties be obliged to provide an alternative identity verification mechanism, and what exceptions should be available?

1. **Yes**
2. No

Comment: "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*".

Question 11B Should a public register of Attributes be maintained?

1. **Yes**
2. No

Question 11C Should there be additional restrictions on access to Restricted Attributes?

1. **Yes**
2. No

Question 12A Are there any other safeguards on Biometric information that should be included in the Legislation?

1. **Yes**
2. No

Question 12B Are there any that have been proposed that should be modified or excluded, and if so, why?

1. **Yes**
2. No

Question 13A Do you agree with the proposed approach on Biometric Information?

1. **Yes**
2. No

Question 13B Will the limitations on Biometric information overly constrain innovation or rule out legitimate future use cases?

1. Yes
2. **No**

Comment: We have previously noted that we commend the approach taken in the paper to restrict biometric authentication to one-to-one queries, as well as the requirement that biometric information be deleted by Accredited Participants after it has been used for the purpose for which it was provided. However, the language in the example regarding a user comparing their voice against a voiceprint held by their credential service provider gives us pause. We are unsure if this conflated centralised credential storage (which we recommend against) with localised limited storage and authentication. We strongly recommend against any framework that allows or encourages centralised biometric databases.

Question 14A Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?

1. **Yes**
2. No

Question 14B Should the Legislation specifically provide an opt-out mechanism enabling individuals to opt-out of the system after they have created a Digital Identity?

1. **Yes**
2. No

Comment: We appreciate the focus on granular consent. We recommend adding a specific prohibition against linking data without consent - this is partly mentioned in the paper, but with the additional, onerous condition of requiring an element of harm to the linking in order to regard it as prohibited.

Question 17 Should the requirement for a Privacy Impact Assessment (PIA) remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

1. TDIF accreditation requirements
2. **Operating Rules**
3. Legislation

Question 18 In addition to the right to privacy and anti-discrimination in relation to accessibility and disability, how should the Legislation safeguard and ensure the enjoyment of Australians' human rights?

Comments: Digital identity programmes must include in design and implementation sufficient safeguards and mechanisms to respect and protect the digital rights of the users. Failure to contemplate or build in these safeguards should force the shut down of deployment of these programmes, with meaningful restructure to better protect the human rights of users. In our recommendations, we urge decision makers to take action in the areas of governance, privacy and data protection, and cybersecurity. It is imperative that the safeguards - legal, technological, and scheme governance - be adopted holistically, and the adoption of one does not preclude the adoption of the other. While principles and guidance for digital identity programmes are essential and provide direction to various constituents in the development of digital identity systems, each system's specific context and distinct features present unique challenges to human rights that must be resolved. To ensure systems' agility and adaptability, it is essential that any digital identity system is evaluated through a human rights lens during all stages of development and deployment. Human rights impact assessment, ex ante and ex post, should be included in the legislation as a requirement for the system as a whole and the operations of the key stakeholders.

Question 21 Should the Legislation include provisions to enable the disclosure of information in specified circumstances?

1. Yes
2. **No**

Question 30 Should the Legislation specify whether and how audit logs from the system can be used in court as evidence?

1. **Yes**
2. No

Comment: 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.

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

Question 31 Is the proposed approach appropriate to achieve a high degree of consistency of privacy protections?

1. **Yes**
2. No

Question 32 Should the Legislation specifically provide that additional administrative decisions relating to the system be subject to merits review?

1. **Yes**
2. No

CONCLUSION

Thank you for the opportunity to participate in these consultations. We hope to be able to facilitate wider consultations, and also discuss our recommendations in detail. We remain available for any clarification or queries in relation to this feedback.

Yours sincerely,

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

[*This submission has been compiled by Raman Jit Singh Chima with inputs from Naman M. Aggarwal, Asia Pacific Policy Counsel and Global Digital Identity Lead at Access Now, and Ria Singh Sawhney*.]

For more information, please contact **identity@accessnow.org** *or visit* **accessnow.org/whyid**

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.