Digital Identity Proposed Legislation Consultation Paper

Submission by the
Northern Territory Government
to the
Digital Transformation Agency

NORTHERN TERRITORY GOVERNMENT
Department of **CORPORATE AND DIGITAL DEVELOPMENT**

Summary

The Northern Territory Government supports in-principle the Australian Government's proposal to develop legislation to govern effective use of a national digital identity system, providing authority and embedding necessary safeguards. The Northern Territory Government recognises and appreciates the benefits for Australian citizens and businesses in having a consistent, rigorous, and easy to use digital identity system operating across the nation.

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 need to be fully considered and addressed prior to legislation being enacted.

The Northern Territory Government is seeking greater understanding and suitable solutions for core elements of a digital identity system in order to address the NTG's reservations that principally relate to:

- meeting the needs of disadvantaged Australians who lack identity documentation and digital literacy
- costs for relying parties and cost certainty
- interrelationships of legislative frameworks between the Australian Government and State and Territory governments
- community understanding, trust and acceptance

The Northern Territory Government has actively participated in interjurisdictional groups working on the digital identity system design and would welcome the opportunity to continue to contribute as this important work progresses.

Benefits and Risks

The primary benefits of a national digital identity system include:

- Consistency – standard rules and entry requirements for digital services across the nation, making it easier for people to access digital services
- Mobility – enabling citizens and businesses to transact efficiently and with confidence in multiple jurisdictions
- Security – data protections at the same level across systems and jurisdictions (noting this can work oppositely if protections are ineffective)
- Cost – common approach avoids jurisdictions and businesses needing to maintain stand-alone digital identity solutions

The primary risks of a national digital identity system include:

- Non-inclusivity – system may suit some sections of the community and not others, meeting mainstream population needs but not those of smaller cohorts with special needs and circumstances

- Lack of acceptance – low trust in management of personal data and negative views, requiring reassurance and whole of community engagement so that people across Australia in all demographic groups are convinced and confident that a national digital identity system will make their lives better
- Limited or no control – with the system and legislation controlled by the Australian Government and governed through an Australian Government entity, State and Territory jurisdictions will have limited ability to ensure the digital identity system will meet their needs and those of their citizens and businesses into the future
- Costs – charging will be controlled at a Federal level with jurisdictions 'locked-in' or facing considerable (re)investment to opt-out of the national system where needs are not being met or costs escalate

Australians with limited proof of identity

To create a digital identity, proofing requirements under the Trusted Digital Identity Framework require documents such as a passport, driver's licence, birth certificate or Medicare card. In the Northern Territory, there will be instances where people will have difficulty creating a digital identity because they lack key identity documents, impacting their ability to use digital services and readily participate in the economy.

This will be especially relevant for Aboriginal people in remote locations where the incidence of unregistered births outside hospitals is higher than for other groups. Language barriers, with English often the 3rd or 4th language used, and limited understanding of government processes or the necessity of such processes, significantly contributes to the lack of documentation to prove identity. It is common for people in these circumstances to not have passports and not uncommon to be without a driver's licence or other documents.

The Australian Government should consider alternative proofing processes that can be incorporated in the planned digital identity system to accommodate such situations and ensure all Australians are able to create a digital identity if they wish to do so. It is understood that this will need to be considered within the context of appropriate safeguards to avoid false identities or stolen identities being registered, however is a priority issue for the Northern Territory.

The Australian Government has adopted the National Identity Proofing Guidelines to verify a person's identity. To highlight local responses to meeting this challenge, the NT Government Motor Vehicle Registry has implemented a more flexible administrative policy that addresses Evidence of Identity challenges in regional and remote communities through, in addition to the nationally accepted forms of ID documentation, also accepting NT-specific IDs, such as those issued by local councils and Aboriginal entities, and having a Non-standard Evidence of Identity verification process in place.

Interactions with state and territory laws, policies and programs

How the proposed Australian Government legislation and its supplementary operational rules would interact with the legislative frameworks in place in states and territories is unknown and not covered in the consultation paper.

Reference is made to privacy legislation, with the interaction between states and territories and Commonwealth privacy laws already established. There may be an intention to establish a similar model for the new legislation, with Commonwealth and states/territories legislation designed to co-exist and work together, although this is not currently clear. This is an important matter of jurisdiction that will be of particular interest to State and Territory governments.

There could be a risk that if the NT laws are not assessed as equivalent, participating agencies and users will be subject to different privacy laws, only for the purposes of this legislation. Further clarification around the legislative impact is required as the implications for the NT Government will need to be considered carefully.

Information is sought on planned implementation of the digital identity system across jurisdictions, particularly interactions with different governments and legislation to facilitate a truly 'tell-us-once' approach and advice on how digital identity mobility will be managed across Australia.

Opt-in/Opt-out

The consultation paper makes it clear that citizens will have the choice to opt-in to the national digital identity system and can opt-out at their discretion. This position is strongly supported, although some practical difficulties are likely to emerge, particularly once the system has been operational for some time.

The consultation paper acknowledges that some smaller private organisations may not be able to provide alternatives to an online digital identity (eg paper-based identity). It appears likely that there will be other organisations that make having a digital identity a condition of dealing with them. In these situations, digital identity verification is not entirely voluntary and may exclude people from accessing services.

The consultation paper is silent on the position for relying parties, including governments, and the extent to which relying parties have choice and discretion. The proposed legislation will establish new authority for the Australian Government and set new obligations on relying parties. The extent to which relying parties can opt-in or opt-out of the national digital identity system is not stated. The ability for relying parties to change this decision in the future, including any impacts or restrictions, is not known.

A clear opt-out process needs to be established to allow relying parties to readily withdraw from the national digital identity system with minimal financial and administrative liability.

Charging framework

The consultation paper outlines a charging framework that will be set and administered by the proposed Oversight Authority, with charges covering costs of the authority and fees for accredited service providers. This presents a scenario where cost efficiency is not incentivised and charges for relying parties are very likely to increase. Relying parties have no influence on the charging regime and limited options to withdraw (relying parties will be largely 'locked-in' to a single supplier model with the Oversight Authority).

There are acknowledged cost efficiencies for relying parties, including governments, in accessing a national digital identity system through removing the need to establish and maintain their own identity systems. As a national digital identity system is continued over time, the balance between costs avoided and charges levied has strong potential to change and leave relying parties exposed to higher ongoing costs.

The charging framework needs to be set having regard to the flow-on costs to relying parties and the potential for cost increases as usage grows with higher transaction volumes and more services digitised. The proposed charging framework should be premised on a focus of maximising benefits to users and the economy and incentivising usage, with relying parties involved in setting charges, strict rules and public justification for any increase in charges.

The NT Government requires clarification and further details in relation to the proposed charging framework.

Community acceptance

There is substantial history in Australia of well-intentioned national initiatives that require citizen data failing or falling well short of expected or required community take-up, despite extensive public communications programs and well understood, sound purposes for most. Examples extend from the proposed Australia Card in the 1980s, to the myHealth record and more recently the COVID safe app. The examples highlight that, while digital take-up and expectations of 'tell-us-once' have increased dramatically, the underlying perspectives and trust of the Australian people have not changed appreciably for decades.

All Australian governments, through the then Australian Data and Digital Council, agreed to adopt a set of Trust Principles to guide government actions as they design citizen services. These overarching trust principles of respect, security, accountability and transparency should be at the heart of a national digital identity system; without citizen trust and confidence in using the identity system, the scheme will fail.

The Australian Government can take advantage of lessons learned from earlier 'trust the government' initiatives and do things differently with the proposed digital identity legislation to present a compelling and believable case to the Australian people. An open compact between government and the Australian people is needed and will require substantial and sustained effort to deliver. The consultation paper does not cover in any detail how this will be achieved and what will be done for community engagement to achieve the success that has eluded other national public communication programs.

Concluding comments

The Northern Territory Government supports the concept of a national digital identity system, while highlighting a number of critical areas that need to be worked through prior to the passage of any legislation, including:

- supplementary methods of identity verification for Australians with limited proof of identity

- interactions with state and territory legislation and policies, along with clarification of jurisdictional boundaries and responsibilities
- securing the trust, confidence and support of the Australian people to take-up the digital identity system and stick with it
- alignment with the Australia Data and Digital Council Trust Principles
- choice and discretion available to relying parties in using the digital identity system
- functions and powers of the proposed Oversight Authority
- charging framework and future cost 'captivity' for relying parties
- mechanisms to facilitate 'tell-us-once' seamlessly across jurisdictions

The Northern Territory Government welcomes the opportunity for further collaboration to resolve these issues and implementation challenges and to participate in designing a system that will meet the needs of all Australians.