Digital Identity Roundtable

NAB recently convened a roundtable of leading thinkers in the field of digital identity. Experts from industry, Government and academia were present and each generously shared their insights and unique perspectives. With the benefit of these insights, NAB is facilitating a journey towards collaboratively co-designing the Australian digital identity ecosystem.

This discussion was anchored around topics, including:

- Privacy, security and customer centricity;
- Plurality of digital identity systems; and
- Access and Inclusion.

As the discussion was held under the Chatham House Rule, comments in this summary are unattributed.

Please note that the opinions expressed herein are the personal views of the roundtable participants and do not necessarily reflect the official views of the organisations represented, including NAB.

Summary

Five key themes emerged in the discussion (which we outline further below):

1. **Identity and Identification.** Individuals rarely need to prove their *identity*. Rather, in most cases, they need to prove they possess an attribute for a particular purpose (i.e., I am over 18 years old and therefore legally allowed to purchase alcohol, or I am a licensed fisherperson and entitled to fish in these waters).
2. **Data minimisation is a crucial ingredient for the ecosystem.** At its core, "privacy is about restraint" and we need to curb overcollection, oversharing and over retention of data at every stage in the data life cycle.
3. **Navigating the options should be simple and seamless.** The onus should not be on consumers to assess which solutions best meet their needs, and to encourage adoption of these solutions, different systems must work effortlessly with one another.
4. **For economic sustainability and choice, government and private sector offerings are key.** In Australia, we have the freedom to decide whether we are 'consumer' or 'citizen' in different contexts, and a plurality of systems upholds this value and contributes to the economic sustainability of any infrastructure.
5. **Data sharing imports notions of power and culture.** It is therefore paramount that these systems are truly voluntary and are designed with the reality and lived experience of all parts of our community in mind.

The themes and observations from participants are further described below.

1. Identity and Identification

The concepts of 'digital identity' and 'digital identification' are often conflated, causing confusion; one participant noted that "identity is too big a word for what we're doing and is not helpful." In most cases an

organisation or agency's interest is not actually in an individual's identity, but rather in verifying a particular attribute or eligibility.

This labelling problem pervades both the private and public sector, as 'digital identity' solutions and programs are said to provide individuals with the ability to "prove who they are," however, it is very rare that individuals need to prove who they are.

For instance, there are many things which people are permitted to do without the government needing to know who they are, and these could be viewed as forms of 'permissions,' or 'authorisations,' for example whether a person holds an authorisation to provide financial advice; to drive a car; or to fish in a certain area.

Instead of couching this as an issue of identity, we should use terms such as identification or verification, which are more germane to the problem we are trying to solve. This reframing will assist in how we design the ecosystem: what do we need to know about an individual for a particular purpose?

2. Data minimisation is a crucial ingredient

Such a framing aligns well with the concept of data minimisation, which is an essential ingredient of the ecosystem.

There are different standards of verification required for different use cases. For example, where an individual is purchasing something online, there is little interest in knowing who they are, versus if an individual is opening a bank account or being employed to do a certain job, where a higher standard of verification or identification may be necessary.

Ultimately, there is a need for more rigour around what information we collect and for how long it is retained.

One participant described "we over-collect for a variety of reasons. One reason is that the thing that we really need to know, for example, the credit card number is no longer reliable on its own, because these are all on the black market and so therefore, we collect other identity information to verify this. It's like pouring gasoline on the fire."

Some sectors of the economy have entrenched beliefs about what they need to know and requirements to hold on to this information. Equally, retention may be based on high levels of risk aversion, from perceptions or greyness in regulations on required information and retention periods. This underlines our collective responsibility in building better literacy regarding data protection and privacy, to help support data minimisation.

It was noted by one participant that we need to differentiate between the "rules, regulations, the 'lore' and the law," which underpin these behaviours. Whilst there was unanimous agreement that data minimisation was a worthy goal, there was also a call to action for regulation to align with this goal and encourage this objective.

Where most have focused on 'user centrality' and user control, this was challenged. It was noted that additional data can be used constructively in healthcare analysis and other research areas (though only by those with highly specialised knowledge and training), and it is important that there is robust data governance in these settings, with data use being in line with the user's consent.

3. Navigating the options should be simple and seamless

Whereas global interoperability is an eventual goal of such a framework, in the first instance we need to ensure that the ecosystems work seamlessly within our own borders.

For this, we need to take a broad view across other developments happening right now, for example the Consumer Data Right and the *Data Availability and Transparency Act 2022* (Cth). As the challenge of adoption already looms large, consent frameworks must be effortless for users across these ecosystems and not add unnecessary friction.

In pursuing an interoperable identification ecosystem, we must be flexible to the practical realities of different account types (e.g., bank accounts and energy accounts). Authentication requirements vary markedly across sectors, and it was noted that there is "complexity at the architecture and engineering level to build interoperable standards, and as such working on these concurrently with any rules is likely to be beneficial."

Other jurisdictions may provide examples from which we can learn, for e.g., Europe's eIDAS has taken a pragmatic approach in not trying to harmonise entire systems, but instead harmonising "end-points," opening up more opportunities for cross-border trade.

4. For economic sustainability and choice, government and private sector offerings are key

On the question of whether public and private sector each have a role to play in bringing a digital identification framework to life in Australia, the answer was a resounding yes.

One participant illustrated the point through an analogy, noting that "the state is an important player in the game but is also the referee and therefore cannot play every single position because they will get tired out." Economic sustainability of the ecosystem is therefore maintained where private sector also contributes to its creation and ongoing development.

Comparison was also drawn to financial market infrastructure, where the core system, which is integral to the economic stability of Australia is operated by the state, with the remainder of the ecosystem being built by the private sector, oversighted by government where the systems connect. As such, there are rules of the road for the ecosystem to operate within.

The notion of choice was reiterated and permitting the private sector to play a role in an identification ecosystem reinforces an individual's right to choose. Upholding this right also reflects the fundamental characteristics inherent in our legal system, culture and Australian society, more generally. Whether Australians wish to use private or public identification infrastructure should be their choice, and their preferences may change over time.

It was also underscored that the private sector's role is broader than verification and each of government and the private sector must ensure the overall safety and cybersecurity of the ecosystem and provide support to consumers and citizens, if something goes wrong.

The importance of quality credentials throughout the lifecycle of a transaction was also emphasised. For example, in the case of a drivers' licence, the state has a role to play at the outset in ensuring that credentials are verified and there are no duplicates or false drivers' licences in the system. Thereafter, if a licence is compromised this will have a downstream impact for transactions using that credential and therefore there needs to be an information exchange between ecosystems to flag and address these issues.

5. Data sharing imports notions of power and culture

A key theme that permeated the discussion was the way in which concepts of identity, and information exchange import notions of culture and power. As we are living in social structures, individuals are trusted or gain access based on 'social signaling' or social determinants. While this may be reflective of existing societal norms and constructs, it should be questioned whether it is desirable to perpetuate them in digital form.

Equally, it was clear from the discussion that in creating the ecosystem, our goal should not be to merely digitise the analogue identification documents that exist today. Instead, we should actively look for opportunities to

extend and better cater to those who are not well served by current frameworks today. One participant also spoke of issues associated with racial profiling and exclusion, which the use of biometric technologies can entrench in systems, whilst appearing objective.

Experience was shared of Māori culture, in which identity links back not only to ancestral lines but also to connections with mountains and rivers. It was noted that jurisdictions such as New Zealand are actively considering how to embed Māori cultural knowledge in the design of digital identity trust services legal frameworks and within businesses processes. It was acknowledged that where cultural worldviews are considered, systems are more likely to work well for everyone.

Another participant spoke of the concept of "digital self-determination, as the ability to transition to self-determination digitally and make informed choices" in the context of First Nations Australians and this theme extended to an all-encompassing position that we need to ensure that no parts of our community are locked out from accessing opportunities in an increasingly digitised economy. Equally, we also need to recognise that there will be individuals and cohorts who do not wish to use digital identification systems and we need to ensure that use of these systems is truly voluntary in nature. It was cautioned that if we do not address inclusion in the system from the start, then we risk excluding the people who are already the most vulnerable.

Actions and next steps

From the discussion, the following calls to action emerged:

- **Bring clarity to the nomenclature to accurately frame the problem statement.** This is well within our power and each of us have a role to play in distinguishing between the concept of digital identity and digital identification or verification, where the latter more precisely defines our goal and the boundary around what information is needed, in each context.

- **Data minimisation strategies need support** through regulation, for example by government streamlining and clarifying record retention requirements in legislation and through business processes, where the private sector should move towards a world of zero knowledge proofs (i.e., it is enough that I know you are over 18 years old, I do not need to also collect your date of birth).

- **Harmonise the connections and endpoints, so they work together effortlessly.** We should heed the experiences of regulatory frameworks elsewhere, supporting a range of user experiences, which can seamlessly operate across different use cases.

- **Embed a cultural lens across these solutions and frameworks *ab initio*** to promote self-determination and agency. If we do not design inclusion in the ecosystem from the start, it will further entrench disadvantage and exclude access to opportunity for those who are already the most marginalised.

NAB is committed to doing our part to pursue these calls to action.

To transform these discussions into more tangible initiatives, we will also be launching a 'design sprint' to further develop what a future interoperable Australian digital ID ecosystem might look like, and to identify the gaps in our current landscape and invite expressions of interest in relation to these activities. We are also committed to helping to upskill and grow greater literacy on the potential benefits associated with a safe and interoperable digital identification ecosystem within the Australian community, including in relation to data minimisation, increased productivity and improved access to services.