TELSTRA CORPORATION LIMITED

Response to Digital Transformation Agency Consultation Paper: Digital Identity Legislation

Public version

23 December 2020

CONTENTS

EXECUTIVE SUMMARY

Telstra welcomes the opportunity to respond to the Digital Transformation Agency's (**DTA's**) consultation on the legislative framework and governance structures that should be put in place to support an expanded Digital Identity system in Australia (**Consultation**).

Telstra considers that government leadership in the rollout of and adoption of digital technology to save individuals time and money and help businesses and government improve efficiency and productivity is essential to broader uptake of digitisation. The scale of the opportunity that accelerated digitisation presents to rebuild the economy is significant. In new research conducted by PwC for Telstra[1], it estimates that increased digitisation will add up to $90 billion to the Australian economy and create 250,000 new jobs, all by 2025.

Digitisation will be important for enabling Australia to be a leading digital economy by 2030[2]. As government services move online, Australians will be able to access government services from anywhere at a time convenient to them over their preferred channel. Businesses will have more flexibility and be able to expand their reach to more customers locally and globally. Choice, convenience and need will drive Australia as a digital economy: although to realise full benefits requires keeping Australian citizens, businesses and governments safe online. Once the framework is in place, the expanded Digital Identity system will be a key enabler to this outcome.

COVID-19 has been a powerful catalyst to accelerate change. Technology and connectivity will be central in helping countries adapt to post-COVID working and living, as well as realising many new economic and social opportunities that arise from profound disruption. People all around the world rapidly embraced digital experiences like never before – whether it be working from home, doing their shopping, consulting their doctor, exercising, or watching a concert, and research indicates they are not planning to stop. The way forward is a digital economy.

As a result, Telstra has seen a dramatic uplift in Australian businesses and government services needing to transform at pace and taking enormous leaps when it comes to their digital transformation. We're supporting customers to deliver complex transformation projects in days, or weeks instead of months or years. For Telstra, COVID-19 accelerated our use of digital tools for customer interaction. Many customers now connect with us through self-service and online tools such as messaging. Before COVID-19, around 50% of consumers contacted us through digital options, now it's over 70%. We've also seen almost 4 million customers download the My Telstra app during COVID-19 in just 8 weeks[3].

It is absolutely the right thing for the DTA to be looking at ways in which we as a country can consolidate on this momentum to make it a permanent trend, and to enable transacting online to occur safely. Government and regulators have a significant role to play in enabling the nation to capitalise and build on this momentum, as well as ensuring digital inclusion so all Australians can benefit from digitisation.

With one in every 14 people working in government[4], delivering services Australians rely on every day, we agree with the DTA that there are real opportunities to be found in further enabling government at all levels to embrace the digital economy and advance its digital journey. We see this journey including the scaling of digitised and responsive government services, digital integration and automation of processes and facilities, providing staff and customers with tools for remote collaboration, and the leveraging of data analytics and artificial intelligence (**AI**) to deliver better, faster and more efficient services.

With the right framework in place to ensure choice, trust, privacy, security and encourage adoption, we see an expanded voluntary Digital Identity system in Australia as a valuable tool sitting alongside other

[1] See https://exchange.telstra.com.au/unlocking-businesses-90-billion-digital-potential/

[2] https://www.pm.gov.au/media/digital-business-plan-drive-australias-economic-recovery

[3] See https://exchange.telstra.com.au/making-self-service-easy-with-the-new-my-telstra-app/

[4] Australian Bureau of Statistics, Labour Force Australia, October 2020.

identity establishment, verification and management options to help transform citizen engagement and democratise frictionless access to services by enabling more government and business services to move online, creating win-win outcomes for users and participants alike.

We are therefore pleased to share in the body of this submission some of our intial thoughts on key focus areas for the Digital Identity legislative and governance framework, which we believe will be important to its success. We would also welcome the opportunity to continue to engage with the DTA as it further develops its thinking and shares exposure drafts of the intended legislation and other instruments to support rollout and adoption.

01 Safeguards

Ultimately, the Digital Identity system will not succeed in delivering the desired productivity and efficiency outcomes unless users have confidence and trust in the system, hence are comfortable to, and appropriately protected in, using it. Further, this situation of trust must extend not only to sophisticated users, but also to more vulnerable user cohorts.

We agree with the DTA that this requires the right legislative and policy safeguards to be established. The DTA should also consider how Government can collaborate on public engagements or education campaigns that build Australians' understanding of, and trust in, digitisation more broadly. Below, we offer some initial observations on some of the key areas we consider should be addressed.

1.1. Choice

Telstra supports federated identity management, leaving control in the hands of citizens and consumers to choose which government agencies and commercial entitites can access their information and for what purpose. Using a digital identity won't suit everyone, and it will be very important for government and business participants in the system to understand how citizens and customers like to engage. It is, therefore, critical that the proposed legal digital identity framework remains voluntary.[5]

It is also important that entities in scope for expanded participation in the system retain flexibility to adopt the approaches to identity verification and management that best suits their individual needs. Telstra currently peforms substantial digital and non-digital identity verification/management for our customers, both to comply with applicable legislative and regulatory requirements, and as part of our processes designed to minimise fraud and to ensure that existing verified identities are managed securely.

It is of vital importance that the new framework does not add regulatory burden and complexity for business or government, by creating parallel mandatory sets of requirements for relevant vertical segments, such as the telecommunications industry.

In this context, it will be equally important to ensure that the framework is technology-neutral and platform-agnostic, as well as principles-based to the largest extent possible, to cater for the immense variety of sectoral and technological approaches to identity verification and management. For example, it would be impractical for telecommunications service providers to use the system if it required them to take consumers out of an embedded digital flow (i.e. integrated through API's or SDKs).

It will also be important that choice is left in the hands of users of the Digital Identity system as to which digital identity service provider they use based on their individual preferences, as well as having absolute control as to if, when, by whom and how their digital identity can be used in each case.

Overall, Telstra believes that now is the right time to think differently about customer service in the future, and we are optimistic that getting the framework right to support expanded rollout and adoption of the voluntary Digital Identity system will give participants more capacity to serve customers requiring more complex support, and for those customers who are not as comfortable using digital tools.

1.2. Security

The framework must be developed cognisant of the growing cyber risk presented by more and more people doing more things online, creating the opportunity for those with ill-intent to take advantage. The Prime Minister recently raised awareness of the significant, sophisticated and ongoing cyber attacks against Australia including by a state based actor. We are also seeing significant increases in cyber crime targeting Australians and Australian businesses.

[5] It would not in our view be consistent with this principle, if it were open to businesses or government agencies to insist a consumer established a new digital identity or used an existing one, in order to deal with them / obtain certain services. In addition, such practices may raise accessibility and discrimination concerns.

In fact, the increasing volume of compromised credentials Telstra is seeing associated with identity documents such as government issued Australian Driver's licences means that we are now needing to expend significant efforts to check the validity of documents, in addition to verifying that the identity credentials are owned by the person asserting that identity.

Just recently, Telstra announced our pilot with Services Australia, to identify and reject illegitimate text messages that appear to be sent from myGov and Centrelink to Telstra customers. With the support of the Australian Cyber Security Centre, Telstra completed a technical proof-of-concept using metadata to identify and reject illegitimate SMS traffic spoofing using Telstra SenderIDs on our network. This initiative focusses in particular on SMS Scams where scammers impersonate known and trusted brands, like Telstra, Australia Post, Centrelink, banks and others, to redirect people to malicious websites.

The only way to look at cyber security is as a team, because we are all connected online. We welcome the Government's strong engagement with industry in development of its 2020 cyber security strategy and look forward to this collaboration continuing. It is also important that Government is an exemplar in protecting its own systems and in building its own capability – and this is very much true for the planned expanded Digital Identity system. It should be expected and prepared for that attribute and credential service providers, identity exchanges and providers and also relying parties and users themselves will be the subject of attacks and fraud.

Not only will stringent adherence to Trusted Digital Identity Framework (**TDIF**) accreditation obligations on security be important, but also education and awareness for users and relying parties on cyber safety and identity protection measures – explaining best practice for the safeguarding of sensitive information and reducing the risk that staff, the community and partners expose identity data through irresponsible actions.

Particularly as the reach and use of the system grows – we also recommend that special focus is given in the framework to the ways in which one form of digital identity may be used to establish another – especially if that new form of digital identity is of a higher level of assurance, allowing it to be relied upon for transactions of increasing significance for the user and the relying party. While identity theft and fraud may be easier and more prevalent with identities at lower levels of assurance, it is critical that such false identities cannot then be used to create false identities at higher levels of assurance. For trust to be achieved in the overall scheme, it is key that when a user moves between different assurance levels, this is done in a secure and consistent manner across identity providers.

1.3. Privacy

Telstra supports the importance placed on privacy in the design of the framework. However, we also support the response of Communications Alliance to the Consultation on the importance of harmonising the privacy requirements in the Digital Identity framework with existing requirements of the various sectors, as well as other overarching legislation such as the *Privacy Act 1988* (**Act**), to allow and incentivise future participants to join the system with ease and without unnecessary expenditure.

We note the Consultation's reference to the ongoing review of the Act. Currently the Act already allows for different levels of protections for ordinary personal information compared to sensitive personal information. If there are other categories of information which, by their nature may attract additional risks, we recommend these are covered under the framework of the Act. Similarly, the instances in which disclosure of personal information provided under the system would be permitted should be covered under the framework of the Act. Having different levels of privacy protection for similar data, such as has been created in the consumer data right (**CDR**) datasets and some telecommunications data covered by Part 13 of the Telecommunications Act 1997, creates unnecessary complexity and confusion.

1.4. Restrictions on data profiling

Telstra supports the restrictions on data profiling proposed in the Consultation, including the proposed restrictions on behavioural profiling. We consider the proposed restrictions and prohibitions to be very important to protect the integrity of users' information, and to promote trust in the system.

1.5. Consent

Consistent with our submissions above on the critical importance of user choice, Telstra wholeheartedly supports the system being built around user consent.

In this regard, we consider the legislation should explicitly provide a mechanism requiring an individual's consent before a user transacts with a relying party. Further, we consider that the requirements for de-enrolment need to be included in the legislation, to ensure identity service providers do not maintain identity data after the consumer has requested this be removed. There could be a specific requirement for deletion or destruction, although we believe that the general requirements under the Act for personal data to be deleted/destroyed when there is no longer a permitted purpose for holding it would apply.

1.6. Age

The Consultation rightly notes that a range of issues must be considered when it comes to the setting of minimum age requirements.

Some of these issues may be able to be resolved by considering the age appropriate level of assurance that may be asserted, with younger users being more limited in the level of assurance (i.e. points of ID) that may independently be asserted.

When it comes to informed consent of a user (such as to enrolment), it is vital that the consent is valid. This may in some cases appropriately involve a guardian of the user. However, consideration should also be given to specific cases such as victim survivors of domestic family violence, where no parent or guardian is available.

1.7. Acting on behalf of another

We support the framework contemplating the need for users to obtain the assistance of another person to engage with the system, or to do so on their behalf – such as putting in place requirements to allow representatives to act under a Medical Power of Attorney.

02 Governance and sustainability

2.1. Legal authority for expanded use

Telstra supports the proposed expansion of the Digital Identity system, so it is able to be used by non-Commonwealth entities, including the private sector and states and territories, and so that different identity service providers may be accredited to participate in it.

2.2. Financial sustainability of the system

We agree that adoption of an appropriate charging framework will be important to the sustainability and utilisation of the Digital Identity system.

We recommend that consideration is given to alignment of the charging framework with the level of assurance required by the relying party, and volume of the consuming organisation. To ensure a competitive and consistent environment across different identity providers, we also agree with the proposal that the charging framework is overseen by a central governing body.

2.3. Independent governance and oversight

Trust in the expanded framework by users will be key to its success. It will be of vital importance for users to know that their personal information is safe, and can only be used in the way they authorise. In this respect, we support the response of Communications Alliance to this consultation, highlighting the importance of a governance and oversight body that is truly independent – and, importantly, is also perceived to be independent.

2.4. Record keeping and other regulatory requirements of participants

Along with regard to record keeping obligations of participants, we recommend consideration is also given to related and/or other relevant regulatory requirements of participants / potential participants – such as the requirements for records auditability which apply to telecommunications providers under the *Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017*.

2.5. Liability

The liability framework for the system will have an important bearing on its adoption by Participants, relying parties and users, and it will be key that the right balance is struck in the case of conflicting interests. Particularly for potential new identity service providers contemplating joining the system, it will be important for them to understand the underlying liability associated with their identity assertions for any given level of assurance requested. It is also important to understand the emerging impact of the security landscape and for government to consider a liability framework that ensures protection of users, and also organisations.