COMMUNICATIONS ALLIANCE LTD

Communications Alliance submission

In response to the

Digital Transformation Agency

Digital Identity Legislation Position Papers

- **Governance of the system**
- **Liability framework**
- **Administration of charges for Digital Identity**
- **Scope of the legislation and interoperability with other systems**
- **Privacy and other consumer safeguards**

17 March 2021

Contents

1. Introduction

Communications Alliance welcomes the opportunity to provide a submission in response to the Digital Transformation Agency's (DTA) five Position Papers on the development of the Digital Identity legislation:

- Governance of the system
- Liability framework
- Administration of charges for Digital Identity
- Scope of the legislation and interoperability with other systems
- Privacy and other consumer safeguards

Our members welcome any efforts aimed at contributing to voluntary enhanced security mechanisms in relation to identity establishment, verification and management. In fact, our members in the telecommunications sector already undertake substantial digital and non-digital identity verification/management for consumers of communications services, either against the background of legislative and regulatory requirements and/or as part of their own processes, designed to minimise fraud and to ensure that existing verified identities are managed securely.

As enablers of large parts of Australia's digital life, our members naturally take a keen interest in any systems that allow their organisations and their customers to further enhance their digital experiences while simultaneously safeguarding privacy and maintaining security.

Against this background, we offer the following comments.

2. Identity fraud and security

If successful, the implementation of the Trusted Digital Identity Framework (TDIF) will increase the use of digital identities (IDs) by Australians substantially. Eventually, the use of a digital ID will become the norm. For the TDIF to build trust, it is key that fraudulent identities are not created and that each verified identity is indeed representing the person that they purport to be. If a fraudulent identity is introduced into the system, we foresee two major problems. Firstly, trust in the TDIF will be irrevocably eroded, and secondly, the scale of the new system has the potential to amplify consequences of fraudulent IDs and/or ID theft.

Therefore, we urge Government to reassure itself whether all necessary and possible measures have been taken to minimise the risk of identity fraud 'at the front end' prior to taking any steps that are likely to amplify the already existing risk of identify fraud.

We are concerned that none of the Position Papers appears to stipulate a specific level of security or compliance with a security standard as a prerequisite for accreditation or participation in the TDIF. We note that the Office of the eSafety Commissioner, in cooperation with major industry players, academia and other relevant stakeholders, has developed Safety-by-Design principles that emphasise "the need to address online harms, alongside user safety and rights, in the product development lifecycle so that safety is systematically embedded into the culture and operations of organisations"[1]. Similarly, the Australian Cyber Security Centre's Cyber Security Principles, could be used to develop similar principles for a Security-by-Design approach for the TDIF.

Against this background, we propose that it may be useful to add to the role of the Oversight Authority by allowing it to set standards and practices for a Security-by-Design approach.

[1] https://www.esafety.gov.au/about-us/safety-by-design

3. Liability

It appears that the liability arrangements will be key to entities' considerations whether to (voluntarily) participate in the system. It is, therefore, critical that potential entrants understand all possible liability scenarios prior to making their decision. To this end, we recommend the DTA provide sufficient case studies and examples covering various scenarios under the proposed liability regime, including examples involving cyber incidents.

Further guidance will also be useful on how liability is envisaged to be allocated where fraudulent IDs are involved. Similarly, further thought may need to be given with respect to liability in scenarios where participants of the system rely on incorrect information published on the Oversight Authority Register. This may become relevant where parties rely on the Register as proof whether a transaction is subject to the ID legislation and where, through some error or time delay, the Register does not accurately reflect the correct status of a participant.

Moreover, the Position Paper *Liability and redress framework* states:

> "It is proposed that, once a participant is onboarded following accreditation, it will be subject to a statutory multilateral contract. Any other participant or user who suffers a loss as a consequence of the actions of the participant can enforce that contract against the participant. All that would be required to determine liability would be for the participant or user to establish the loss and that the participant failed to comply with the statutory rules."

However, without further details on the terms of the contract and whether it is envisaged that participants would have an ability to limit (and to what extent) or to exclude liability in certain circumstances, we find it very difficult to provide more detailed feedback at this stage.

4. Privacy regime

With a view to the future uptake of a voluntary framework, it will be important to harmonise the requirements of the framework with existing requirements of the various sectors as well as other overarching legislation such as the *Privacy Act 1988* to allow and incentivise future participants to join the framework with ease and without unnecessary expenditure.

End-user trust will also be conditional on a transparent and clearly understood privacy framework.

Therefore, we are concerned with the aspects of the Position Paper *Privacy and other safeguards* that foreshadow a dual privacy regime for States and Territories:

> "State and territory government entities participating in the system as accredited participants will now have greater ability to adhere to local privacy legislation instead of federal privacy law. The new policy is designed to provide greater flexibility and autonomy for state and territory agencies, align with other federal legislation, and make it easier for state and territory government entities to participate."

In a world of ever-increasing mobility of users and data, allowing States and Territories to choose which privacy law (State vs Federal) they adhere to appears to be moving in the wrong direction and ought to be avoided as it introduces unnecessary complexity for participants in the system and potentially also confuses users of the system.

We also note with concern that the *Privacy Act 1988* is currently under review. While the Position Paper seeks to assure stakeholders that "the proposed Digital Identity legislation will not duplicate or conflict with established principles in existing legislation"[2], we remain concerned that the revised *Privacy Act 1988* may contain changes that may not align well with the digital ID framework. We believe that it would be prudent to delay the final

[2] p. 6, Position Paper *Privacy and Other Safeguards*, Digital Transformation Agency, March 2021

development of the privacy regime of the Digital Identity legislation until after the review of the *Privacy Act 1988* has concluded.

5. Ministerial powers to create rules

The Position Papers propose that the legislation contain significant scope for the Minister to make rules. For example:

p.7 Position Paper Liability Framework:

> "It is proposed that the legislation would enable the Minister to make legislative rules that would provide limitations on liability in response to emerging issues once the system is rolled out and bedded down."

p.14 Position Paper Scope of the legislation and interoperability with other systems

> "The responsible Minister will have the power to make rules necessary for the register on the recommendations of the Oversight Authority, who will determine what will be included in the rules."

p.17 Position Paper Scope of the legislation and interoperability with other systems

> "It is proposed the Minister will have the power to add new roles in rules and provide for additional roles to be added to the registers to provide transparency on the entities performing new roles."

We understand that it may be appealing to create a 'bare bones' legislative framework with the intention to allow for a greater degree of flexibility and to potentially make necessary adjustments once the legislation has been enacted. However, allowing the Minister to make substantial parts of the framework through subordinate instruments removes powers from the ordinary legislative process and ought only to be considered where absolutely necessary, rather than be the default solution to any difficult issue.

In any case, we believe that prior to making/changing any rules, or assigning any new roles, the Minister ought to be required to publicly consult for at least 28 days. Any resulting instruments ought to be disallowable in Parliament.

6. Conclusion

Communications Alliance looks forward to further engaging with the DTA and all relevant stakeholders in this important process, to create an effective and efficient expanded voluntary digital identity framework for Australia.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507