Digital Transformation Agency (DTA)

Submission on proposed Digital Identity legislation - *The DTA is seeking the public's views on proposed legislation that will support an expanded Digital Identity system in Australia.*

Summary / About Yoti

1. This response is made on behalf of Yoti Australia Pty Limited (ABN 49 634 795 841) a wholly owned subsidiary of Yoti Holdings Ltd (registered in England and Wales with company number 09537047) and Yoti Ltd (registered in England and Wales with company number 08998951) together referenced in this submission as "*Yoti*".

2. Yoti owns and operates a free digital identity app and wider online identity platform that allows organisations to verify who people are, online and in person. This could be using the Yoti app, which allows individuals to share verified information about themselves on a granular basis or it could be using Yoti's 'embedded' services which allow organisations to add a white label identity verification flow into their website or app. It could also be using Yoti's authentication algorithms such as facial recognition, age estimation, voice recognition or lip reading.

3. Yoti has a team of around 230 based in London, with offices in Bangalore, Los Angeles, Melbourne and Vancouver. There have been over 9.5 million installs of the Yoti app globally, following its launch in November 2017. Similarly, over 400 million checks have been conducted using Yoti age estimation service since February 2019.

4. Yoti holds the ISO 27001 certification and continues to be audited every year. Further, Yoti is annually certified to SOC 2 Type 2 for its technical and organisational security controls by a top four auditing company. The SOC 2 standard is an internationally recognised security standard. Yoti also holds the Age Verification Certificate of Compliance, issued by the BBFC. Yoti is certified to the publicly available specification PAS:1296 Age Checking.

5. If there are any questions raised by this response, or additional information that would be of assistance, please do not hesitate to contact Yoti at:
   Darren Pollard
   Regional Director Australia
   darren.pollard@yoti.com

   Julie Dawson
   Director of Regulatory & Policy
   julie.dawson@yoti.com

   Samuel Rowe
   Legal & Policy Associate
   samuel.rowe@yoti.com

6. Yoti is happy for this response to be published.

QUESTIONS

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

7. Yoti believes that Australian privacy law provides a sufficient legal framework for the protection of Australian residents' privacy. Enshrining further values in primary legislation could prevent the 'rules of the road' from being amended and updated in tandem with technological and social changes.

8. Instead, Yoti encourages the DTA to enshrine relevant privacy safeguards in the Trusted Digital Identity Framework ("TDIF"). There, such safeguards will be more easily amended if technology and social values shift.

Q6 - 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?

9. In Yoit's opinion, the Legislation does not need to include a definition of digital identity as this could fail to capture relevant systems and would preclude digital identity platforms from innovating on what personal data they can retain.

10. For that reason, and the sake of consistency across legislation, the Legislation does not need to include a definition of Digital Identity Information.

Q7 - What factors should be considered in the development of a charging framework for the system?

11. Yoti agrees with the principles of charging relying parties rather than users, since relying parties derive savings from the use of digital identity and extract revenue from users. Users should not be charged for using their digital identity by either the digital identity platform or the relying party.

12. However, Yoti questions whether a single charge should cover all Participants' activities. Different activities incur different costs for the digital identity platform. For example, it can be more expensive to perform address verification than to perform document verification.

13. In order to encourage competition in the market, digital identity providers should be able to price their offerings competitively. Having a single charge for all activities would preclude their ability to do so.

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

14. In Yoti's view, Participants should be held liable for fundamental breach of contract leading to damage and when it can be proved that damage has been suffered as a result of the Participant's negligence.

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

15. Yoti recommends that a digital identity ombudsman is considered as a method of enacting redress for users under the trust framework.

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

16. As stated in response to question 6, Yoti considers the existing legal framework sufficient for protection consumers and their data from misuse by Participants.

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

17. Yoti considers that mandating rules concerning the extent of choice available could be a good way of avoiding discriminatory outcomes, which might not otherwise fall within the ambit of Australia's anti-discrimnation laws.

18. However, Yoti cautions the Australian government from creating a legislative system that is overly prescriptive and forces relying parties to provide secondary methods of verification where they are clearly unnecessary.

Q 11A - What types of profiling of behavioural information should be prohibited and allowed?

19. In Yoti's opinion, profiling and behavioural information should be limited to the following two purposes:
    a. to assist product development of identity verification systems
    b. to assist the analysis of which demographics are and which are not able to use digital identity verification, for the purpose of increasing accessibility.

Q 11B - Should a public register of Attributes be maintained?

20. This appears to be a good idea in principle. However, Yoti is unsure how it would be put into practice, given that it would need constant updating and maintenance. The public confidence it might engender could be considerably lower than the resource taken to run the register.

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

21. Because Restricted Attributes are often crucial to effective identity verification, it seems strange to Yoti that additional restrictions would be placed on accessing them. For example, document numbers can contain a formula, which acts as a document security feature.

22. Yoti does not recommend creating additional restrictions on access to Restricted Attributes.

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

23. Because of the legal protections already provided by the Privacy Act, Yoti questions what further would be achieved in practical terms by writing further legislation on the use of biometrics.

24. Instead, Yoti suggests that the regulation of the use of biometrics by Participants be enacted through the trust framework rules. In that way, they will be more easily amended to keep up to date with emergent technologies.

Q 13A - Do you agree with the proposed approach for Biometric Information?

25. Yoti agrees with the proposed approach, aside from the creation of new legislation, as discussed above.

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

26. Yoti suggests that DTA gives extensive thought to what is meant by the word "consent" and the legal connotations it has. Services will often rely on a user verifying or authenticating their identity. Therefore, relying parties will want to prevent users from interacting with their service where the user refuses to verify or authenticate their identity.

27. Consent implies that there is an alternative where the user refuses to provide their consent. However, that is not how identity transactions work.

28. Yoti therefore suggests that DTA replaces "consent" with approval, since approval does not contain the same implication of an alternative mechanism.

29. If DTA continues to rely on consent, Yoti suggests that many relying parties will be unable to meet the requirement and use digital identification. That would render the entire trust framework useless.

30. There are numerous other legal bases that could be relied upon by identity service providers

Q 15 - Should there be a minimum age set for a person to be permitted to create their own Digital Identity? If so, what should it be?

31. Yoti encourages the DTA to consider how, in practice, a young person may create their own digital identity without input or ongoing oversight of a parent or guardian.

32. Further, the DTA may wish to take into account the age at which individuals can permit the processing of their personal data as a relevant factor when deciding if there should be a minimum age for a person to create their own digital identity.

Q 17 - Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

33. For the reasons set out in the consultation document, Yoti believes the requirement should be placed in the Legislation.

Q 21 - Should the Legislation include provisions to enable the disclosure of information in specified circumstances? If so, what should those circumstances be?

34. The Legislation should only require that disclosure of information takes place if the two following tests are met.

35. First, that a law enforcement request has been made to access the information.

36. Secondly, that access to information is, at the very least, technically feasible. In addition, Yoti would recommend that the request be proportionate, clearly articulated and relevant to a crime.

Q 27 - Should the record keeping requirements be outlined in the Legislation? If so, what should they be?

37. Yoti does not consider that the record keeping requirements should be outlined in the Legislation. Those requirements would be better placed in the trust framework rules. This is so that they can be amended easily, keeping pace with technological advancements that may occur.

38. The Privacy Act already creates a sufficient legal framework, mitigating the need for the creation of new law to sit alongside the Archives Act.