Yoti Ltd: Fountain House, 130 Fenchurch Street
London, EC3M 5DJ United Kingdom

Yoti Australia Pty Limited: Level 2, 696 Bourke Street
Melbourne, Victoria 3000 Australia

Wednesday 27 October 2021

Mr Jonathon Thorpe
General Manager Digital Identity and myGov
Digital Transformation Agency
50 Marcus Clarke Street
Canberra ACT 2601 Australia

Via submission: www.digitalidentity.gov.au/have-your-say/phase-3/submission-form

Australian Trusted Digital Identity Legislation
Trusted Digital Identity Bill 2021
Phase 3 Consultation Response - Yoti

Dear Mr Thorpe

On behalf of Yoti, we appreciate the opportunity to provide our submission to Phase 3 of the Consultation with the DTA in respect to the Digital Identity Legislation and the proposed Trusted Digital Identity Bill 2021.

Summary / About Yoti

1. This response is made by 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 350 based in London UK, with offices in Bangalore, Los Angeles, Melbourne and Vancouver. There have been almost 11 million installs of the Yoti app globally, following its launch in November 2017. Similarly, over 500 million checks have been conducted using the Yoti age estimation algorithm since 2019.

4. Yoti holds the ISO 27001 certification and continues to be audited every year. Further, Yoti is certified to SOC 2 Type 2 for its technical and organisational security controls by KPMG. 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:

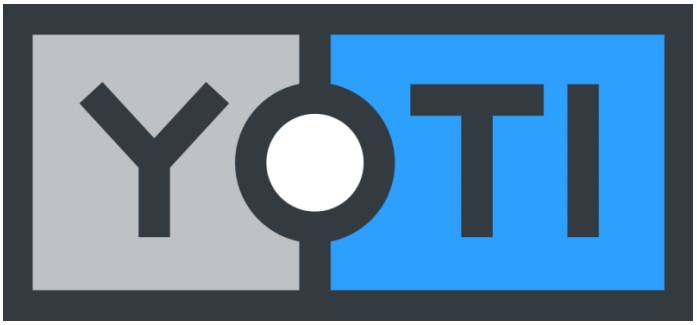
   Julie Dawson
   Director of Regulatory & Policy (UK)
   julie.dawson@yoti.com

   Darren Pollard
   Regional Director Australia
   Director - Yoti Australia Pty Limited
   darren.pollard@yoti.com

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

Yours sincerely,

Darren Pollard
Regional Director Australia - Yoti Ltd
Director - Yoti Australia Pty Limited
Email: darren.pollard@yoti.com



Yoti's response to the public consultation on Australia's Digital Identity Legislation

Trusted Digital Identity Bill 2021

Phase 3 - 27 October 2021

Respondent(s) full name(s):
Julie Dawson, Director of Regulatory & Policy
Darren Pollard, Regional Director Australia

Email address(es):
julie.dawson@yoti.com
darren.pollard@yoti.com

Contact phone number:
+44 2030 583 463

Organisation submitting the response:
Yoti Australia Pty Limited
ABN 49 634 795 841
Level 2, 696 Bourke Street
Melbourne Victoria
3000 Australia

www.yoti.com

Contents

Yoti Feedback to the Trusted Digital Identity Bill 2021

Section 10 - Meaning of attribute of an individual

Yoti would challenge the presence in (3) of an individual's criminal record. We believe it should be considered an attribute of an individual, as it could form part of required background checks in certain use cases such as the delivery of visas or employment checks. Yoti would suggest making a clearer distinction between the existence of a criminal record, and individual criminal convictions, their duration, and whether they have been served or not.

Section 17 - Applicants may be required to enter into trusted provider agreements

Yoti would welcome clarity on the form that the 'trusted provider agreement will' take? The Bill provides little detail on this. This is a key document for the whole ecosystem.

Section 18 - Approval to onboard to the trusted digital identity system

Yoti would welcome the inclusion in this section, at (5) (a) in the case of a refusal, and (6) in the event of an approval, of an additional duty for the Oversight Authority to share such decisions with the entities that have already been accredited to the trusted digital identity system.

Section 20 - Minister's directions regarding onboarding

In (2), Yoti would welcome more clarity on both the process for appeal and the time for appeal when an entity receives an instruction from the Oversight Authority that their accreditation to the digital identity system has been suspended.

Section 22 - Conditions on approval to onboard to the trusted digital identity system

In (4), Yoti would welcome more clarity on whether the Australian Government considers this clause empowers the Oversight Authority to impose further conditions on onboarding to the trusted digital identity system after an entity's onboarding date.

Section 24 - Variation and revocation of conditions

Yoti would welcome more clarity in this section about the amount of time an entity would be given to comply with a variation on one or more conditions to approval as decided by the Oversight Authority.

Section 25 - Notice before changes to conditions on approval

Yoti would welcome clarity in (2) (a) about whether it is intended for the notice to be public, and how it is to be given to the entity.

Yoti would also welcome more clarity in (2) (b) about how the Oversight Authority may decide what an appropriate period of time would be for an entity to provide a written statement relating to the proposed condition, variation or revocation.

Yoti would also suggest that this notice include a proposed date by which the entity should comply with the proposed condition, variation or revocation.

Section 26 - Notice of decision of changes of conditions on approval

Yoti would welcome more clarity in (3) (a) on how the Oversight Authority is to determine what a reasonable deadline would be for an entity to comply with a new condition, a variation or a revocation.

Section 27 - Applying for a variation or revocation of conditions on approval

Yoti would welcome more clarity on how entities can apply for such variations or revocations, and in particular whether this can be done using the existing TDIF Exemption Request Form.

Section 28 - Suspension of approval to onboard to the trusted digital identity system

In (5) (b), Yoti would welcome more clarity on whether the show cause notice given to an entity by the Oversight Authority will include a deadline by which the Oversight Authority has to make a decision by, following reception of an entity's written statement.

In (9), Yoti would welcome more clarity on whether the revocation of an entity's suspension applies from the day that the notice of revocation is given.

Section 29 - Revocation of approval to onboard to the trusted digital identity system

Yoti would welcome more clarity in (2) and (6) (c) about the criteria that the Oversight Authority would use to determine when the revocation of an entity's approval should take effect.

Similar to the previous section, Yoti would welcome the inclusion in (4) (b) of provisions to help entities determine the amount of time the Oversight Authority will need to consider an entity's written statement and make a final decision.

Section 30 - Generating and using a digital identity is voluntary

Yoti would welcome the inclusion in (1) of examples of alternative pathways relying parties should be required to offer individuals as a condition of providing a service or access to a service.

Yoti would welcome more clarity in (7) (a) about the format a request for exemption with regards to providing a service or access to a service should be in.

Section 31 - Holding etc. digital identity information outside Australia

In (1), the Bill creates a lack of certainty in the law by granting to TDI the authority to rule on whether data can be held outside of Australia. It would be helpful if a decision was made on this point and stated in the law.

Further, (2) does not include a clear list of the grounds the Oversight Authority must consider in exercising its discretion under section 31. This would provide useful clarity and also a means of challenge if TDI were to exercise its authority in a detrimental manner.

In (2) (b), Yoti would welcome more clarity on whether entities can apply for such exemptions and how, and whether the Oversight Authority may revoke these exemptions, and what processes this would require, particularly in terms of the time required by the Authority to repatriate data held outside of Australia.

Section 34 - Exemption from interoperability obligation

Yoti would welcome more clarity in (3) and (5) about what processes would need to be followed to revoke an interoperability exemption, including to challenge this decision, and the amount of time an entity would be given to comply.

Section 35 - Trusted provider agreements

As stated previously, Yoti would welcome clarity on the form that the *"trusted provider agreement"* will take.

Section 37 - Entities may conduct testing in relation to the trusted digital identity system

Yoti would suggest that in (2), there should be more clarity about whether such an application for authorisation should specify the type of data the entity wishes to retain to conduct testing, and whether an entity can also ask to hold data outside of Australia via the same request.

Section 38 - Use and disclosure of personal information to conduct testing

Yoti would welcome clarity on whether this Bill proposes to create mechanisms allowing the Oversight Authority to revoke an authority for an accredited entity to use or disclose personal information of an individual. If so, Yoti would also welcome further information on whether there would exist mechanisms such as those existing in previous sections (such as a 28 days window to appeal).

Section 39 - Accredited entities onboarded to the system protected from liability in certain circumstances.

Yoti would prefer to see either or both of (i) an aggregate limit on liability for Identity Service Providers and Attribute Service Providers so that Yoti could seek insurance against this figure; and (ii) a fixed penalty sum for each fraudster who bypasses an ISP / ASP's systems due to the ISP / ASP's fault. The current liability model outsources all liability, with an uncapped amount, from relying parties to ISPs and ASPs in the case of negligence or omission by the ISP or the ASP. This clause will make it difficult for ISPs and ASPs to source insurance.

Section 43 - Redress obligations of accredited entities

Yoti would welcome more clarity in this section on steps ISPs would have to take when there is a fraud or cyber incident, etc.

Section 53 - Variation and revocation of conditions of accreditation

Yoti would recommend the insertion in (2) of a new (c) section on the use of age assurance technology in the trusted digital identity framework. We propose adding (c) 'matters relating to age assurance technologies, of which age estimation and age verification are subsets.'

This duty should be accompanied with a requirement for the Oversight Authority to internally review and assess how age assurance technology can support all citizens both with and without access to identity documents to simply prove their age.

Yoti would suggest that the Oversight Authority be required to engage and consult with key emerging technology industry members to better assess how age assurance technology not yet included or considered in the framework can be assessed. This would support the Government's objective to offer consumers a wider choice of IDSPs. Engagement with industry experts can also ensure the Oversight Authority benefits from the latest and most relevant insights.

There are several clear use cases for this technology, which could be taken into account when assessing an entity's capacity to deliver important regtech solutions and meet respective IDSP levels.

These cases may include age estimation as an age assurance method to access social media platforms as proposed by the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) and the Online Safety Act 2021 (Cth), or state or territory legislation such as recent Liquor Amendment (24-hour Economy) Bill 2020 (New South Wales) which mandates digital age verification for the online purchase of alcohol with same day delivery.

This would also help the Government to achieve its aim (as stated in Section 30, (1)) that there be no requirement for an individual to generate or use a digital identity to receive a service or have access to a service.

We attach to this consultation an appendix (Appendix A) which includes more information on the potential benefits for the trusted digital identity framework of considering and using age assurance technologies. We would also be delighted to provide the Government and Members of Parliament more information and technical demonstrations of our range of age assurance solutions

Section 57 - Suspension or accreditation and Section 58 - Revocation of accreditation

In sections, Yoti would welcome more clarity on whether suspension is immediate from the day that an entity has received the Oversight Authority's written notice, or whether there would exist a 28 day window to appeal this as in other possible interactions between the Authority and entities.

Section 60 - TDIF accreditation rules may incorporate etc. material as in force or existing from time to time

Yoti would welcome the inclusion in (1) of a duty for the Oversight Authority to inform entities at the earliest possible time of the upcoming 'adoption or incorporation' of 'instruments' or 'other writings' if they create more requirements for entities to follow.

Section 61 - Digital identities must be deactivated on request

Yoti would welcome more clarity on whether it is the Government's aim that, if a request has been received, the user's attributes and digital identity should no longer be usable but retained, or deleted entirely.

Section 75 - Prohibition on single identifiers

As a general rule, Yoti would warn the Government against allowing an accredited entity to assign a unique identifier to an individual within a digital identity system at all, unless it is for

the purposes stated in (4) (a), as this may eventually allow for user tracking and could undermine public confidence in the scheme.

Section 76 - Restrictions on collecting, using and disclosing biometric information

Yoti would suggest the addition of (1) (c) to allow entities, and in particular Identity Service Providers, to collect and use (not disclose) biometric information if consented by the user for research purposes and in order to contribute to the reduction of gender or race based bias among others.

Section 79 - Deletion of biometric information of individuals

Yoti would welcome the inclusion in (3) of a mechanism, as in previous sections, allowing entities to request that the Oversight Authority grant an exemption from these requirements, especially in the form of a longer retention period than specified in (3) (b).

Section 117 - TDIF accredited entities register and Section 118 - TDIS register

In Sections 117 and 118, Yoti would welcome clarity on whether the register as described in (1) and the details listed in (2) will be freely accessible by members of the public.

Appendix A - Age Estimation

To date, age verification has solely been considered as a subset of identity verification with the framework. We concur that age can be a subset of identity and can be proved by those owning an identity document, or in a data minimised way through identity verification or digital identity apps.

However, age estimation technology has also evolved to enable people who may not own, have access to or do not wish to use an identity document to prove their age, or that they are over or under a certain age, in a privacy preserving manner.

We therefore recommend that the Oversight Authority should further consult with Identity Service Providers to develop a better understanding of how they can deliver TDIF's existing IDSP Levels, trust and privacy objectives by using age assurance. That consultation should recognise the valuable role of both age verification and age estimation methods.

We would also recommend that the Oversight Authority gather input on the standards and approaches already available in the market and that it consider how age should be treated for each IDSP.

We think there are obvious benefits in expanding the scope of the framework to include age estimation (distinctively from age verification), such as helping the Oversight Authority achieve the stated social and economic objectives as defined in Chapter 3 - Objects (1). This inclusion would also help to future proof the Bill, and ensure Australian consumers can have access to more streamlined services - for example at the point of sale for the purchase of alcohol.

Use cases and policy aims

Many areas of the economy will benefit if privacy protecting age checks are made available to consumers, such as the retail, gambling, and online content sectors among others. This would also represent an opportunity to create a broader, standardised Australian approach to age assurance.

The inclusion of the technology to provide age gating at 13+/-, 18 +/- in the framework would allow the Bill to support the Government's wider policy aims of preventing underage access to age restricted goods and services and enable the design of more age appropriate online services. This would ensure younger citizens can make the most of the digital world and thrive online.

Australia would be world leading if it took this proactive stance and could avoid many downstream discussions across multiple government departments, if each one has to work out ways to undertake age assurance.

International comparisons

The Digital Identification and Authentication Council of Canada (DIACC) has been considering creating a specific profile for age under DIACC, called 'anonymous identity attributes', as no personal information is required. DIACC are considering other attributes which also fall into this category, such as location.

The EU Consent Project is reviewing interoperable approaches to age verification and parental consent.

There are ten countries around the world who are reviewing age gating approaches to regulate access to adult content: Canada, France, Germany, Ireland, Italy, New Zealand, Philippines, Poland, South Africa and the UK.

In the United Kingdom, there are currently two regulatory sandboxes reviewing aspects of age. The Home Office Sandbox is reviewing innovative age approaches for the retail of alcohol, including age estimation technology at check-out terminals. The ICO Sandbox has been preparing solutions for the new Age Appropriate Design or Children's Code. There is also a proposal for a scheme specifically for age, within the DCMS Trust Framework.

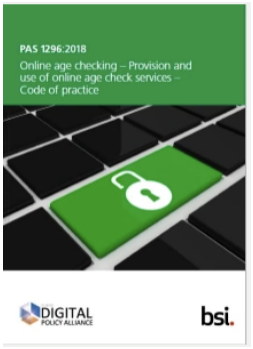
US Senators have written openly to the tech platforms requesting them 'to extend to children and teens in the United States any privacy protections you implement in the United Kingdom'. Childrens' Codes have also been developed in Ireland and the Netherlands.

Minimum Age Assurance Standards have also been proposed in a Private Member's Bill [1]by Baroness Kidron and are soon passing to the Third Reading stage in the House of Lords.

Technical standards

1. The British Standards Institution, BSI, published a standard, widely adopted by the age verification sector and a requirement for the UK market. It is titled "Online age checking. Provision and use of online age check services. Code of Practice" and is also known as PAS 1296:2018. It was designed to be agnostic across goods, services and age, providing tokenised, data minimised approaches to age checking.

[1] https://bills.parliament.uk/publications/41683/documents/325



2. The International Standards Organisation has also accepted a proposal from the United Kingdom, supported by the Department for Digital, Culture, Media and Sport, to define an I**SO** standard for age verification. This builds upon the PAS 1296:2018.

PWI 7732 – Age Assurance Systems Standards is based on the presentation and recommendations arising from ISO SC27/WG5. A working draft will be ready by the end of 2021. Yoti serves on the drafting committee. It spans both age verification and age estimation approaches.

Minimum Age Assurance Standards have also been proposed in a Private Member's Bill by Baroness Kidron and are soon passing to the Third Reading stage in the House of Lords.

Transparency, accuracy and evaluation

In order to enhance public support and trust between various entities in the framework, Yoti would also recommend that the Oversight Authority, having expanded the scope of TDIF to include age estimation, should encourage Identity Service Providers to publish their Mean absolute error (MAE) rates.

Yoti periodically publishes and updates its white paper on age estimation. The latest, October 2021 version for the first time includes results for estimating children under or over 13.

This would also help the Government justify its just decision to allow entities to use biometrics data for testing purposes. This would be one more reason why it should consider our previous recommendation that the aim of testing, together with an increase in the time data retention is allowed, should also be to reduce racially and gender based bias

Yoti would also welcome a requirement for Identity Service Providers to offer independent auditing of its age estimation technology, systems and testing. Potential organisations that could undertake this review include:

- Defence Science and Technology Group (DSTG), a division of the Australian Department of Defence (https://www.dst.defence.gov.au/discover-dst/about-dst)
- Age Check Certification Services Pty Ltd (ABN 66 640 499 921) a wholly owned business of Age Check Certification Scheme (https://www.accscheme.com/about