Response to Consultation Paper on proposed Digital Identity legislation

Anonymous submission

Before completing your submission you will need to read the Privacy Notice. I have read the above Privacy Notice and understand how my personal information will be used, and I wish to continue.	**Yes**
Can we publish your submission?	Yes, but I prefer to remain anonymous. Your submission will appear on our website with the name 'Anonymous' in place of any name or organisational name you provide.
I am submitting:	As an individual
Q16. Question 1A Are the matters (legal authority, privacy protections, governance, amendments) relevant matters which should be included in the Legislation? Take me to the relevant part of the Consultation Paper | Section 3.1 Purpose of the Legislation	**Yes**
Q19. Question 1BAre there additional matters which should be considered? Take me to the relevant part of the Consultation Paper | Section 3.1 Purpose of the Legislation	Yes
Q20. If yes, please give more information about what additional matters should be considered?	Citizen preference. There are citizens, like myself, who do not wish to have a Digital Identity. We should have the right to chose, as we do for taxation matters, to not have a digital presence.
Q22. Question 2AWhat matters covered by the TDIF should be incorporated into the primary legislation? Take me to the relevant part of the Consultation Paper | Section 3.2 Structure of the legislative framework Please tick all that apply:	other (please specify)
Q23. What other matters should be incorporated into the Legislation?	Citizen choice.
Q24. Please describe why you think the selected above, including other, is important	The underlying assumption throughout the legislation is that people who do not want a digital identity / presence are criminals,or undertaking criminal / illegal behaviours. That is simply wrong. There are people like me who want to avoid a digital footprint as much as possible, particularly a digital ID, and do not find the conveniences or benefits, such as they are espoused, worth the intrusion and exposure we feel. Experiences like myGov, and the numerous data breaches that we were assured could never happen, do not instil any confidence in the proposed legislation. If you examine the number of active myHealthRecord and COVIDSafe app accounts, you will see that there is far less than a 70%, never mind 100%, uptake of these digital services. That should be an indicator to you of a proportion, a large proportion, of the Australian public's attitude to being 'forced' into a digital 'product'. Do not forget the AustraliaCard push of a few (?) decades ago. This is, by any measure, AustraliaCard by stealth, and

	the attitudes of a large number of Australians, myself included, to that and any antecedents, no matter how packaged, has not changed.
Q25. Question 2BWhat matters covered by the TDIF should be incorporated into Operating Rules? Take me to the relevant part of the Consultation Paper | Section 3.2 Structure of the legislative Framework Please tick all that apply:	other (please specify)
Q26. What other matters should be incorporated into the Operating Rules?	Again, citizen choice.
Q27. Please describe why you think the selected above, including other, is important.	See previous comments
Q28. Question 2C What matters covered by the TDIF should remain as policy? Take me to the relevant part of the Consultation Paper | Section 3.2 Structure of the legislative framework Please tick all that apply:	other (please specify)
Q29. What other matters covered by the TDIF should remain as policy?	Citizen chpoice.
Q30. Please describe why you think the selected above, including other, is important	See previous comments.
Q31. Question 3Is a publicly available 'Digital Identity Participant Register' an appropriate mechanism to communicate who will be covered by the Legislation? Take me to the relevant part of the Consultation Paper – Section 3.3 Scope of the Legislation	No
Q33. If no, please give more detail about why a publicly available 'Digital Identity Participant Register' is NOT an appropriate mechanism to communicate who will be covered by the Legislation?	It goes firmly against privacy principles. Any register at all.
Q34. Question 4Are the proposed obligations on relying parties described [see link] reasonable? Take me to the relevant part of the Consultation Paper – Section 3.3 Scope of the Legislation	No
Q36. If no, please give more detail about why the proposed obligations are NOT reasonable?	Again, citizen choice.
Q37. Question 4[second part] Should there be any additional obligations in addition to the proposed obligations on relying parties?Take me to the relevant part of the Consultation Paper – Section 3.3 Scope of the Legislation.	Yes
Q38. If yes, please describe what additional obligations should apply	Alowing citizen choice for participation. And not an "opt out" rule, but an "opt in" rule.
Q40. Question 5Are the concepts outlined [see link] appropriate to include in a definition of 'Digital Identity' for the Legislation? Take me to the relevant part of the Consultation Paper – Section 3.3 Scope of the Legislation.	Yes
Q52. Question 8CWhat remedies and/or redress should be available to aggrieved Participants and Users for loss or	By saying that "Multiple Participants are involved in the verification of a natural person's identity and there is no single point of accountability/responsibility" and "It is possible a Participant or User

damage suffered as a result of their use of the system? Take me to the relevant part of the Consultation Paper – Section 3.5 Liability	could suffer loss or damage as a result of their use of the system, notwithstanding every other Participant acting in compliance with the system's rules and requirements. It is proposed that Participants would not be liable for loss or damage in such circumstances" is not good enough. It allows for damage to occur, responsibility to be avoided, and redress to be unavailable. In designing the system you should consider a central, formalised, final "insurer of last report" upon whom damages and responsibility in such circumstances could be attributed. It could mirror the ComCare system, with participants paying a levy to cover loss and damages attributed to the central entity.
Q53. Question 8DWhat other best practice mechanisms and processes should be considered to support Users when things go wrong? Take me to the relevant part of the Consultation Paper – Section 3.5 Liability	Automatic, no fault and no cost, rebuilding and redress of digital identity if the User desires.
Q57. Question 9BAre additional protections required? If so, what? Take me to the relevant part of the Consultation Paper – Section 4.2 Privacy	Yes
Q58. If yes, please explain what additional protections are required	The scheme must be voluntary for users. The comment "These privacy and consumer protections could include: ensuring the system remains voluntary, not mandatory" must be changed to "MUST include OR enshrine".
Q60. Question 10AShould the Legislation include rules around the extent of choice available to Users to verify their identity? Take me to the relevant part of the Consultation Paper – Section 4.3 Choice	Yes
Q61. If yes, please explain why the Legislation should include rules around the extent of choice available to Users to verify their identity	Yes. The "opt-out" clause for so-called lesser services opens the door for any service to make a Digital Identity mandatory. This is not acceptable, and the obligation on relying parties to provide an alternative mechanism must be legislated.
Q63. Question 10BShould any types, or all types of relying parties be obliged to provide an alternative identity verification mechanism, and what exceptions should be available? Take me to the relevant part of the Consultation Paper – Section 4.3 Choice	Yes
Q64. What exceptions should be available to provide an alternative identity verification mechanism?	Grounds of religion, personal conviction, physical / mental inability (and I'm not being condescending, there are many conditions that will prevent this), and also where the recording of any digital identity would present a threat to personal or national security (yes, I'm serious, thinking of women who have AVOs / DVO against violent partners, or people working for ASIO/ASIS/DSD etc where there anonymity is critical). By the same measure, there may also be a need to specify who should not be able to use an alternate identity verification mechanism. Perhaps people who have committed and been convicted of identity theft or fraud.
Q66. Question 11AWhat types of profiling of behavioural information should be prohibited and allowed? Take me to the relevant part of the Consultation Paper – Section 4.4 Restrictions on data profiling	This "It is proposed that the Legislation will prohibit the creation of a single identifier for individuals that is used across the system" should be enacted.
Q67. Question 11BShould a public register of Attributes be maintained? Take me to the relevant part of the Consultation Paper – Section 4.4 Restrictions on data profiling	No
Q71. If yes, please explain why there should be additional restrictions on access to Restricted Attributes?	This restriction "The Oversight Authority will only grant access where the User has consented to the release" should be legislated.
Q73. Question12AAre there any other safeguards on Biometric information that should be included in the Legislation? Take me to the relevant part of the Consultation Paper – Section 4.5 Biometrics	Yes
	Again, citizen right to not have a digital ID or Biometric information

Q74. If yes, please explain what other safeguards on Biometric information should be included in the Legislation?	stored.
Q76. Question 12BAre there any that have been proposed [see link] that should be modified or excluded, and if so, why? Take me to the relevant part of the Consultation Paper – Section 4.5 Biometrics	Yes
Q77. If yes, please explain which safeguards should be modified or excluded, and why?	Where a User has consented for their Biometric Information to be used, it will only be kept while the permitted purpose still exists" opens the door to extended or indefinate retention. A specific time period should be set when the information is given
Q79. Question 13ADo you agree with the proposed approach on Biometric Information? Take me to the relevant part of the Consultation Paper – Section 4.5 Biometrics	No
Q81. If no, please explain why you do NOT agree with the proposed position on Biometric Information	Safeguards are not suffient. No clear right to opt-out for users, and back-doors have been let open to co-erce participation.
Q85. Question 14AShould the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party? Take me to the relevant part of the Consultation Paper – Section 4.6 Consent	Yes
Q86. If yes, please explain how the Legislation should specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?	An earlier comment I have made highlights that, for some providers, they do not have to provide an alternate channel to a Digital Identity. There is therefore a potential for coercion by Providers choosing not to provide an alternate channel, forcing users into participation. The actions of the ATO, effectively burying the option of a paper tax return and forcing taxpayers to use myGov, when the Senate has made clear that taxpayers can use paper returns, is am example. The opening line that "The system is built around User consent and the Legislation will embed that concept. A User can choose at any time whether they want to use their Digital Identity to access a service, or use an alternative channel" needs to be strengthened in legislation to require Providers to provide a clear, accessible alternative channel that is without prejudice to those who chose to use it,
Q88. Question 14BShould the Legislation specifically provide an opt-out mechanism enabling individuals to opt-out of the system after they have created a Digital Identity? Take me to the relevant part of the Consultation Paper – Section 4.6 Consent	Yes
Q89. If yes, please explain why the Legislation should specifically provide an opt-out mechanism enabling individuals to opt-out of the system after they have created a Digital Identity?	Again, citizen right and choice. The desire of people to "be forgotten" has risen in the wake of global digitisation, and the same should apply here. People should have the right to opt-out and have their Digital Identity erased. Saying that "in such cases, the person's Digital Identity is rendered inoperative and can only be accessed in certain clearly delineated circumstances, such as where it is needed to investigate fraud or other criminal activities" again opens a door for misuse and coercion. Once a person opts out it should be a complete opt-out. Also, the term "other criminal activities" is too broad;

	it allows any activity to be the basis for retention or reactivation of a digital identity, as the definition of criminality can change, and change rapidly. As a (perhaps extreme) example, abortion may not be a criminal offense in NSW at the moment, but in South Australia it still remains partly criminalised. So there is potential for a woman who has been suspected of having an abortion in SA to have her Digital Identity accessed or resurrected against her wishes, whilst if she was a resident of NSW that could not occur. With the evolving nature of the euthanasia debate across Australia, there is even more potential. At the least, the definition of "other criminal activities" should be tightened and defined clearly to avoid such aberrations; at best, opt-out should include mandatory erasure of the Digital Identity with no option of resurrection.
Q91. Question 15Should there be a minimum age set for a young person to be permitted to create their own Digital Identity? Take me to the relevant part of the Consultation Paper – Section 4.7 Age	Yes
Q92. What should the minimum age set for a young person to be permitted to create their own Digital Identity be?	14
Q93. Please explain why you chose that age	I would have preferred to give a range, but looking at the examples, I think the medical treatment/myHealthRecord age is right; it shoud be an age where the person is capable of understanding what they are doing. Under 14 seems too young.
Q95. Question 16How should the Legislation cover situations where a person lacks capacity, is not capable, is too young or lacks interest or motivation to engage personally with the system? Take me to the relevant part of the Consultation Paper – Section 4.8 Acting on behalf of another	In general 4.8 seems ok, but I worry about the intersection of "In some cases, an individual may not be ... willing to engage with the system" and "a nominee may be appointed by ... an individual ... the law ... [or by] relationship ... professional or familial". Again, this opens the door to coercive compliance; An unwillingness to engage should not mean that someone's spouse, accountant, doctor or local police officer can be appointed a nominee to create a digital identity. The potential for abuse exists, and there is no safeguard against it.
Q96. Question 17Should the requirement for a Privacy Impact Assessment (PIA) remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules? Take me to the relevant part of the Consultation Paper – Section 4.9 Privacy Impact Assessments	Legislation
Q97. Please describe why you think the selected above is important	Unless it is legislated, the requirement will have no real force.
Q98. Question 18In addition to the right to privacy and anti-discrimination in relation to accessibility and disability, how should the Legislation safeguard and ensure the enjoyment of Australians' human rights? Take me to the relevant part of the Consultation Paper – Section 4.10 Human Rights	I think your underlying assumption is not supported in the Consultation Paper. It says "the use of a Digital Identity will help to facilitate Australians' enjoyment of human rights, including the right to education, the right to health, the right to social services and welfare payments" which implies that the rights outlined will depend on a Digital Identity. The legislation seems not to safeguard these rights but to exclude people without a Digital Identity from them. The (or any) legislation must explicitly state that a lack of, or decision not to use, a Digital Identity by a User does not abrogate or diminish their rights. As it stands, the legislation as a whole as outlined in the Consultation Paper is drawing up a fresh digital divide between those

	who will have a Digital Identity and those who will not; this in and of itself is an act of discrimination.
Q99. Question 19Is the proposed approach to accessibility and usability practical and appropriate? Take me to the relevant part of the Consultation Paper – Section 4.11 Accessibility and anti-discrimination	No
Q101I.f no, please explain why this is not practical and/or appropriate	See earlier comments.
Q102. Question 19[second part] Should any other considerations be taken into account? Please list them here: Take me to the relevant part of the Consultation Paper – Section 4.11 Accessibility and anti-discrimination	The comment that "facilitating fast and efficient access to a range of services, the system helps to minimise potential discriminatory effects based on age, race, disability, geographic isolation, gender or socio-economic status" is simply fallacious. As I have commented, it is creating a second digital divide, discriminating against people who do not wish to have a Digital Identity.
Q103 Question 20What additional mechanisms, including penalties and redress mechanisms, should be included in the Legislation to prevent disclosure or misuse of personal or other information? Take me to the relevant part of the Consultation Paper – Section 4.12 Penalties	Imprisonment for directors or 'responsible persons'. Financial penalties mean little, particularly where the amounts to be made from misuse are large. Imprisonment however represents a real penalty.