Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
By Email: legcon.sen@aph.gov.au

18 January 2024

Submission: Digital ID Bill 2023

The Free Speech Union of Australia (**FSU**) is pleased to write in response to the consultation on *Digital ID Bill 2023*.

The FSU is a non-profit and non-partisan organisation set up to promote the fundamental human right of Freedom of Speech within Australia. We defend, protect and promote the Free Speech rights of all Australians irrespective of the content of the speech.

We have some substantive concerns about how this Bill will affect Freedom of Expression, which we raise in this submission.

Issue 1: Lack of Safeguards in Respect of Non-Accreditation

Whilst we understand that this accreditation scheme is *notionally* voluntary, there is a risk that it becomes a *de-facto* standard that in practice organisations are required to comply with. Given the onerous nature of establishing an 'ID provider' and maintaining compliance, this is not likely to be open to smaller organisations, who will need to rely upon what will likely be a small number of third-party providers. As this could become essential for running any kind of on-line service in Australia, even an internet forum, or an online store, there is a need to ensure that these ID providers cannot discriminate.

We note that this concern already applies to payment processors, which are a similarly essential digital service. Legal scholars have raised limits on access or denial of access to payment platforms (like Paypal) as being a particular concern for Free Speech.[1] The complexity of providing this service[2] means that there are very few payment processors and limited competition. The result is that it is possible for organisations and individuals to be denied access to this essential service, which is a form of 'debanking'.[3] By way of an example, crowdfunding is a challenge in Australia, the crowdfunding for the Giggle case[4] was removed by at least three different payment processors. We would therefore

[1] See e.g. Balkin, Jack M. "Free speech is a triangle." *Colum. L. Rev.* 118 (2018): 2011.
[2] https://stripe.com/au/resources/more/how-to-create-your-own-payment-gateway
[3] https://www.gov.uk/government/news/tougher-rules-to-stamp-out-debanking
[4] https://www.fedcourt.gov.au/services/access-to-files-and-transcripts/online-files/roxanne-tickle-v-giggle-for-girls

ask the Bill include strong anti-discrimination provisions to ensure that access to accreditation is not impacted by something someone might have said, as well as to remove any chilling effects.

Recommendation 1: There should be a 'cab rank' rule. A provider may not refuse to provide (or discriminate in providing) an identity service to another body that it is able to provide, save on an objective cybersecurity basis which concerns the substantive security of the systems themselves. A person refused service should have the right to apply to the Administrative Appeals Tribunal, which may remove accreditation.

Recommendation 2: Provide strong protections for applicants for accreditation under the 'Digital Identity' regime, limiting criteria for refusal to objective cybersecurity standards encoded in the legislation itself. There should also be a time-limit of no more than three weeks for processing an application, to prevent any stifling by delay.

Issue 2: Unreasonable Limitations on Speech of Cyber-Security Professionals

The Bill unfortunately provides an overly broad protection of commercially relevant information which undermines its very purpose. An ID system can only be trusted if the security processes that it uses are transparent and can be independently validated. The restrictions on communications about system weaknesses mean that security risks are likely to remain undetected, whilst Australia will not be able to recruit the best and brightest security experts to maintain its systems. This also considerably undermines the Free Speech rights of Cyber-Security professionals. An approach based on 'security through obscurity' is not appropriate in the modern era, especially for an identity provider system.[5] Instead, openness should be enforced.

The Bill should be revised to make it clear that disclosing information about the technological operation of systems, or existing security risks, does not attract any penalty. Failing to remove the chilling effect in the Bill will undermine digital ID, by creating systems that appear to be trustworthy, but cannot be trusted in reality.

Recommendation 3: Modify the bill to make it clear that any algorithms, practices and procedures used are **not** confidential information.

If there are any questions with respect to this submission, please direct them to Dr Reuben Kirkham, Operations Director.

Yours sincerely,

Free Speech Union of Australia

[5] See e.g. Yu, Jinying, and Philipp Brune. "No security by obscurity-why two factor authentication should be based on an open design." *Proceedings of the International Conference on Security and Cryptography*. IEEE, 2011.