23 January 2024

Senate Standing Committees on Economics

PO Box 6100
Parliament House
Canberra ACT 2600

Commercial-in-Confidence

Dear Committee Secretariat,

Submission Regarding: Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023

On 30 November 2023, the Minister for Finance and the Attorney General announced that the Digital ID Bill had been introduced into the Senate, a historic step to strengthen and expand Australia's Digital ID System and do more to protect Australians' privacy and security settings in the digital age.

The Digital ID Bill was referred to the Senate Economics Legislation Committee. The Committee is due to report on the Bill by the end of February 2024. Noting that much of the Committee review period is over December and January when people are busy or away, IIS urged anybody with a point of view on the Digital ID Bill to prioritise making a submission.

The Government released an Exposure Draft of a Digital ID Bill in September 2023, aimed at formalising in legislation a digital ID system that has been under development in Australia for many years. IIS Partners made a submission on the 2023 Exposure Draft and a submission to an earlier 2021 Exposure Draft identifying ways in which its protections could be strengthened.

It is gratifying to see many of the suggestions presented in our submission taken up in the Bill as introduced, as discussed further below.

This letter serves as a further submission for the Senate Standing Committees on Economics to consider.

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

Voluntariness

In particular, it has been pleasing to see a strengthening of provisions protecting the voluntariness of digital IDs. Guaranteeing that participation in digital ID systems will be voluntary and non-compulsory is one of the strongest protections available to individuals to avoid overreach by government or other entities and worsening of the power imbalance over individuals.

To that end, our submission raised concern over an exception in the Exposure Draft that would override the voluntary use requirement where 'a law of the Commonwealth, a State or a Territory requires verification of the individual's identity solely by means of a digital ID.' Such a provision, we pointed out, would allow future encroachment on voluntary use. We are pleased to see the removal of that exception from the Bill.

Law enforcement and national security exceptions

Another major area of concern for us was the permissiveness of law enforcement and national security exceptions in the Exposure Draft. IIS has been on the record in a July 2021 submission and again in a October 2021 submission regarding our concern about such exceptions which we find to be too broad, establishing too low a bar for disclosure to these agencies, and too weak a framework for oversight.

With Bill as introduced to Parliament, we see some narrowing of law enforcement exceptions. For example, one of the main clauses enabling disclosure for law enforcement purposes (clause 54) now formally excludes biometric information – disclosure of biometric information for law enforcement purposes is regulated under a separate provision and requires the higher bar of a warrant before disclosure.

We also see that certain exceptions within clause 54 appear to have been narrowed. In the Exposure Draft personal information could be disclosed for law enforcement purposes where the accredited entity was satisfied that the enforcement body reasonably suspected that a person had committed an offence or breached a law imposing a penalty or sanction. In the Bill this has been narrowed to allow disclosure where the accredited entity is satisfied that the enforcement body has started proceedings against a person for an offence or in relation to a breach of a law imposing a penalty or sanction. The penalty for breaching clause 54 has also been increased from 300 penalty units in the Exposure Draft to 1500 penalty units in the Bill as introduced.

The silence in the Bill in regard to national security appears to mean that national security agencies could have untrammelled access to information in the digital ID system through the provisions in other legislation. National security agencies were barred from access to personal information created by the COVIDsafe app, but it seems not here even though the information is just as sensitive.

IIS remains of the view that the Minister's stated goal of 'inclusivity' is likely to be threatened by an overly permissive approach to law enforcement and national security access to information handled and generated by digital ID systems. Law enforcement or national security access has the potential to negatively impact trust in the system which in turn will negatively impact inclusion, especially for individuals who already have a low trust in government or generally on the margins of society.

Funding

It is widely acknowledged that the Office of the Australian Information Commissioner is woefully underfunded for the work it is already expected to do. ACCC also suffers from constrained funding. Initial implementation and continued enforcement of the provisions in the Bill, the foreshadowed subordinate legislation and standards will involve a lot of work.

The two most affected regulatory agencies must be well funded if potential users of the digital ID system are to have any faith in the provisions in the Bill. Without such funding, the protections set out in the Bill will become meaningless, especially because similar digital identity initiatives have failed through lack of trust.

We urge the Committee to recommend in the strongest possible terms that the two regulators be suitably, if not generously, funded in order to create the trust essential to its success.

Looking ahead

In our view, these changes are in the right direction and we will continue to advocate for strict limits on law enforcement and national security access to digital ID system information.

IIS continues to be very engaged in this space with Malcolm Crompton, Founder and Partner at IIS, appointed to the Ministerial Digital ID Expert Panel to provide independent advice on Australia's digital ID program.

We would be pleased to appear before the Committee to discuss the Bill and our submission, if it so wished.

Yours sincerely

Michael S. Trovato
Managing Partner
mtrovato@iispartners.com

Malcolm Crompton AM
Founder and Partner
mcrompton@iispartners.com

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia
www.iispartners.com,

+61 2 8303 2438