

## Introduction

Internet Australia appreciates the opportunity to provide comments on the draft Digital ID Bill 2023.

There are several provisions in the Bill that have the potential to strengthen the ability of Australians to protect their personal information and limit circumstances in which personal information could be required. We also recognise that many Australians will choose not to use a Digital ID and support the clear statement in the Bill that creating and using a Digital ID is voluntary.<sup>1</sup>

There are general concerns with the proposed ID system. A person must have a smart phone, then log into MyGovID to access the Digital ID app. MyGovID was roundly criticised during COVID ID for its security flaws and its difficulty of use. Both those issues must be addressed if the app is to support the provision of a Digital ID. There are other issues if Australians are to adopt a Digital ID including:

- Many people cannot afford a smart phone.
- Many people do not have the skills and confidence to use a smart phone app.
- Many people with disabilities may not be able to use the smart phone app.
- Many people live in regional, rural or remote Australia and do not have access to the necessary transmission capacity.
- The Digital ID is only as secure as the person's smart phone and password.

The approach the issue of Digital Identity outlined in the draft legislation represents a useful start in addressing a significant set of problems. However, until the Government finds ways to effectively address these broader additional issues, the proposed Government approach will be, at best, only a partial solution to these problems and should not be portrayed as anything more than that.

---

<sup>1</sup> Digital ID Bill 2023, Clause 71



# Submission by Internet Australia

---

*Internet Australia has comments on specific provisions of the Bill, as follows:*

## ***Penalty for Disclosure***

Clause 44(4)(e) provides penalties for disclosure of the unique identifier – with exceptions for, inter alia, ‘detecting, reporting, investigating or prosecuting against a law of the Commonwealth, a State or Territory’. This clause is too widely drawn. Laws of the Commonwealth, State or Territory could be for offenses as minor as contravention of a speed limit or minor theft. Disclosure of personal information should only be allowed in the case of contravention of this Act (as is provided) for serious offences of Commonwealth, State or Territory laws.

### ***Recommendation:***

***Clause 44 be amended to either delete Clause 44(4)(e) or limit disclosure of unique identifier information to serious offences with penalties for contravention that include jail terms of up to three years.***

## ***Personal Information Used for Enforcement Purposes***

There is a similar issue with Clauses 51. Again, the prohibition is for use of personal information held by an entity that is used or disclosed for enforcement purposes. Again, the disclosure is allowed if the entity reasonably suspects that a person has committed an offence against a law of the Commonwealth, State or Territory.

### ***Recommendation:***

***Clause 51(a) be amended to either delete the clause or limit disclosure of unique identifier information in relation to serious offences with penalties for contravention that include jail terms of up to three years.***

## ***Civil Penalties***

Clause 56 sets out circumstances in which entities may provide or receive services within the Digital ID System, or otherwise participate in the Digital ID system. Surprisingly, the penalty for non-compliance is only 200 penalty units. Given the need to ensure the competence and quality of all parties to this proposed system, it is not clear why this provision attracts only 200 penalty points when elsewhere in the Bill, non-contravention of requirements attracts 300 penalty unit penalty.

### ***Recommendation:***

***Review penalty units for non-contravention of requirements on all relevant providers of the Digital ID system for uniformity***



### *Compliance Assessments*

Clause 126 provides for the Digital ID Regulator to require assessments of an entity in the system to undergo an assessment to determine if the entity is or is compliant with the Act or if there is or has been any breach of the Act or Rules. Given the importance of an entity's continued compliance with the Act, the outcomes – at least in summary form – should be available publicly.

#### *Recommendation:*

*Amend Division 3 on Compliance Assessments to require that the outcomes of any compliance assessments made by the Digital Regulator are – at least in summary form – publicly available.*

Thank you for your attention.

*Holly Raiche*

*Chair Policy Committee – Internet Australia*

### *About Internet Australia*

Internet Australia is the not-for-profit organisation representing all users of the Internet. Our mission – “Helping Shape Our Internet Future” – is to promote Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our leaders and members are experts who hold significant roles in Internet-related organisations and enable us to provide education and high-level policy and technical information to Internet user groups, governments and regulatory authorities. We are the Australian chapter of the global Internet Society, where we contribute to the development of international Internet policy,

