COMMUNICATIONS ALLIANCE LTD

Communications Alliance submission

In response to the

Department of Finance

Draft *Digital ID Bill 2023*
Draft *Digital ID Rules 2024*
Draft *Digital ID Accreditation Rules 2024*

9 October 2023

Contents

1. Introduction

Communications Alliance welcomes the opportunity to provide this submission in response to the Department of Finance (Department) draft *Digital ID Bill 2023* (draft Bill), *Digital ID Rules 2024* (draft Rules) and draft *Digital ID Accreditation Rules 2024* (draft Accreditation Rules) (and jointly '(draft) legislation and rules').

Our members welcome any efforts aimed at contributing to voluntary enhanced security mechanisms in relation to identity establishment, verification and management. The proposed legislation and accompanying rules, once implemented and embedded within industry and society over time, have the potential to significantly raise the security profile of Australians' digital identity and key pieces of personal information.

As enablers of large parts of Australia's digital life, our members naturally take a keen interest in any systems that allow their organisations and their customers to further enhance their digital experiences, while simultaneously safeguarding privacy and maintaining or improving security.

Consequently, our members warmly welcome the proposed draft legislation and rules. Our feedback below is aimed at providing suggestions for further 'fine-tuning' of the proposed legislation and rules and improved operational effectiveness and practicality.

2. Prohibition of use and disclosure of personal information for certain purposes

Section 52 of the draft Bill prohibits the use of personal information for certain purposes, unless the use of the information is for the provision and/or promotion of the accredited service or the information is disclosed to the individual with the individual's express consent:

52 Personal information must not be used or disclosed for prohibited marketing purposes

(1) An accredited entity must not use or disclose personal information about an individual that is in the entity's possession or control for any of the following purposes:

(a) offering to supply goods or services;

(b) advertising or promoting goods or services;

(c) enabling another entity to offer to supply goods or services;

(d) enabling another entity to advertise or promote goods or services;

(e) market research.

(2) Subsection (1) does not apply to the disclosure of personal information about an individual if:

(a) the information is disclosed to an individual for the purposes of:

(i) offering to supply the entity's accredited services; or

(ii) advertising or promoting the entity's accredited 18 services; and

(b) the information is disclosed to the individual with the individual's express consent.

Note: A person who wishes to rely on this subsection bears an evidential burden in relation to the matter mentioned in this subsection (see 23 section 96 of the Regulatory Powers Act).

In addition, s 31 and 33 state that:

31 Chapter applies to accredited entities only to the extent the entity is providing accredited services etc.

This Chapter applies to an accredited entity only to the extent the entity is:

(a) providing its accredited services; or

(b) doing things that are incidental or ancillary to the provision of those services.

33 Extended meaning of personal information in relation to accredited entities

*To the extent not already covered by the definition of **personal information** within the Privacy Act 1988, attributes of individuals, to the extent that they are in the possession or control of accredited entities, are taken, for the purposes of that Act, to be personal information about an individual.*

Note 1: This section has the effect of extending the meaning of personal information in the Privacy Act 1988 as it applies to accredited entities to mirror the meaning of that term as it is used in this Act (see section 9).

Note 2: This means that the requirements in the Privacy Act 1988 about collecting, using and disclosing personal information under that Act extend to attributes of individuals to the extent that information is in the possession or control of accredited entities. However, this applies only to the extent the information is collected, used or disclosed when those entities are providing their accredited services (see section 31). [emphasis added]

The prohibition of s 52 as drafted does not account for the fact that an accredited entity may have come into possession or control of personal information outside and independent of its activities as an accredited entity. An accredited entity may be in the possession and control of personal information from its customers. This information may, or may not, be identical to the types of information it may be in the possession or control of, as a result of its activities as an accredited entity. For example, as part of its customer onboarding processes, as an integral part of being able to perform its services (such as a phone number) or for any other ancillary reason.

The provisions of s 31 and 33 of the draft Bill (including Notes) also appear to contradict the general prohibitions on use of personal information in s 52(1) of the draft Bill.

To remedy the identified issue, only personal information that the accredited entity has come into possession or control of solely for the purpose of providing the accredited service ought to be covered by the prohibition.

In addition, s 52(2)(b) would need to be amended to read:

(b) the information is used or disclosed ~~to the individual~~ with the individual's express consent.

With these amendments in place, we note that accredited entities that subsequently wanted, or indeed necessarily required, to use personal information in order to provide their primary service (for example, a telecommunications carriage service or an email service which necessarily requires the use of a phone number/email address) would need to seek express consent to use the information provided to it solely as a result of its accredited services.

We also submit that the extension of the definition of personal information in the *Privacy Act 1988* to include technical identifiers, that the Government agreed to in-principle, may further complicate the practical application of this prohibition.

Further consideration ought to be given to this section to ensure that the intent does not impede the necessary and practical uses of personal information of users/customers.

3. One-to-many matching of biometric information

Section 45 (ff) of the draft Bill contains limitations on the collections, use and disclosure of biometric information of an individual:

45 Restrictions on collecting, using and disclosing biometric information

(1) An accredited entity may collect, use or disclose biometric information of an individual only if:

[…]

(c) the collection, use or disclosure is authorised under section 46 or 47; and

(d) unless the collection, use or disclosure is authorised under paragraph 46(3)(a) or subsection 46(5), (6) or (8)—the individual to whom the information relates has expressly consented to the collection, use or disclosure of the biometric information.

Civil penalty: 300 penalty units.

(2) To avoid doubt, and without limiting subsection (1), an accredited entity must not: [emphasis added]

(a) collect, use or disclose biometric information of an individual for the purpose of one-to-many matching of the individual; or

(b) collect, use or disclose biometric information of an individual to determine whether the individual has multiple digital IDs.

*(3) **One-to-many matching** means the process of comparing a kind of biometric information of an individual against that kind of biometric information of individuals generally to identify the particular individual.*

Section 46(8)(c) (subject to criteria being fulfilled) authorises an accredited entity to retain, use or disclose biometric information of an individual if "*the information is retained, used or disclosed for the purposes of preventing or investigating a digital ID fraud incident*".

Against the background of Roundtable discussions (25 Sept 2023) which appeared to suggest that one-to-many matching for biometric information is generally not permissible, we seek confirmation whether the authorisation to use biometric information in one-to-many matching processes and/or to determine whether an individual has multiple IDs for the purposes of preventing or investigating a digital ID fraud incident is indeed permissible.

Furthermore, we highlight that the definition of a 'digital ID fraud incident' does not appear to permit the routine one-to-many matching or use of biometric information to determine whether an individual has multiple digital IDs, as the definition requires the ID being or suspected of being compromised or rendered unreliable. However, we suspect that the routine (i.e. without suspicion) matching of such information, for the purposes of fraud prevention, will be the amongst the most effective tools to detect misuse or fraudulent use of digital IDs.

Against the backdrop of ever-increasing scam and fraudulent activities in the digital ecosystem, we encourage the Government to consider whether further calibration with respect to striking an appropriate balance between fulfilling the legitimate expectations of Australians in relation to their biometric information, and legitimate use cases for such information, could be appropriate.

4. Cyber security incidents

Imminent cyber security incidents

It is important that the national identity system is, to the extent possible, protected against cyber security incidents. It is appropriate that accredited entities comply with the relevant cyber security standards/frameworks and other relevant obligations.

Section 69(b) and (c) of the draft Bill allows the Digital ID Regulator to suspend approval to participate in the system if the Digital ID Regulator reasonably believes that there has been a cyber security incident involving the entity or reasonably believes that such an incident is 'imminent'.

Cyber security incidents are pervasive and can affect almost any entity at any time. The consequences of losing approval to participate in the system are likely to be substantial for affected entities. Consequently, we believe that further specificity is required as to the criteria for considering that an incident is 'imminent', to ensure that the suspension of a participant in the system is subject to objective and well-understood criteria.

Definition of 'cyber security incident'

Further to the above, the definition of 'cyber security incident' is, in our view, overly broad, thereby making it impractical and serving to exacerbate the issue of lacking specificity highlighted above.

Section 9 of the draft Bill defines 'cyber security incident' as follows:

***cyber security incident** means one or more acts, events or circumstances that involve:*

(a) unauthorised access to, modification of or interference with a system, service or network; or

(b) an unauthorised attempt to gain access to, modify or interfere with a system, service or network; or

(c) unauthorised impairment of the availability, reliability, security or operation of a system, service or network; or

(d) an unauthorised attempt to impair the availability, reliability, security or operation of a system, service or network.

Given that neither 'system', 'service' nor 'network' are defined in the draft Bill, the ordinary meaning of those terms must be applied. This means that any of the actions/incidents described in (a) to (d) to systems, services or networks unrelated and ancillary to the provision and/or operation of the entity's systems, services or networks that are being used to provide a digital ID service or to participate in the digital identity system are captured by the definition.

Similarly, the language of s 9(c), as currently drafted, includes 'unauthorised impairments to availability, reliability, security and operation' of the (broadly defined) system, service or network of a participant where such impairments are the result of a power outage, unavailability due to malperformance of software updates (which may not constitute a risk to security) etc.

Consequently, we recommend that the definition of 'cyber security incident' be limited in its application to systems, services and networks that, if compromised, have the capacity to pose a risk to the integrity of the digital ID system. In addition, only impairments that are the result of suspected malicious activity ought to be captured by the definition.

5. Destruction of biometric information

Section 48 requires the destruction of biometric information within 14 days of a request from the individual who is being identified by the information. The 14-day timeframe also applies where the information is being required for the investigation and prevention of digital fraud incidents.

It appears that no exemption to these requirements is being contemplated where law enforcement authorities may wish to access to this information after the 14-day timeframe.

We also note that it may not always be possible to separate the identity verified by biometric information from other information pertaining to the individual or the individual itself that has been identified by the information. This means that the destruction of the biometric information may make further access to other information related to the individual (or even the detection of the individual's existence within an accredited entity's system) impossible, including for law enforcement purposes.

The draft Bill also does not take into account that the data may be required in ongoing claims and proceedings, and should exclude legal proceedings.

Moreover, in our experience, 14 days is a substantially too short timeframe to complete many fraud investigation processes. We recommend a destruction period of 180 days (upon request and subject to the data not being required for ongoing claims and proceedings) be adopted.

6. Additional checks for Relying Parties

The legislation and rules envisage an accreditation process for Identity Service Providers (ISPs), Attribute Service Providers (ASPs) and Identity Exchanges (IDXs) (jointly 'accredited entities'). Communications Alliance supports rigorous accreditation standards for privacy and security to ensure the proposed framework can function appropriately and, importantly, gain and maintain user trust.

However, we remain concerned that the same standards of rigour do not apply to admitting relying parties to the system. While this may be useful to attract relying parties to join the scheme and, therefore, increase reach/breadth, we believe that the current thresholds for

onboarding relying parties may be too low and create the risk for malicious actors to become relying parties in order to avail themselves of user attributes that are envisaged to be available to relying parties under the scheme.

As currently proposed in s 59(1) of the draft Bill, relying parties are required to

- be able to comply with the relevant parts of the Act;
- comply with the relevant parts of the Digital ID Data Standards; and
- meet the requirements prescribed in the Rules, if any.

S 59(2) adds criteria to which the Digital ID Regulator may have regard, such as

- *"matters relating to security (within the meaning of the Australian Security Intelligence Organisation Act 1979);*
- *whether the entity is a fit and proper person"*

"Fit and proper persons" considerations (draft Bill, s 12), in turn, reference the Rules and "any other matters the Digital ID Regulator considers relevant".

Section 7 of the draft Rules specifies a number of requirements in relation to testing, risk assessments, processes and procedures, and business continuity.

We note that express user consent is required prior to enabling authentication to a service (draft Bill, s 42). However, it is conceivable that malicious actors would also be able to elicit such consent from unsuspecting and/or vulnerable users and, subsequently, be able to pursue their malicious activity relatively freely.

None of the criteria and requirements in the draft Bill and draft Rules expressly consider the possibility (and likelihood, so we believe) of malicious actors establishing a business for the purpose of defrauding its customers and who, therefore, could be willing to satisfy the requirements.

Consequently, we submit that relying parties ought to be subject to an additional layer of scrutiny, for example additional checks of a company's history/longevity and its directors. ASIC's criteria for persons it considers 'fit and proper' used for the granting a credit licence may also provide additional considerations that the Digital ID Regulator ought to have regard to (and preferably must have regard to) when assessing relying parties.

7. Liability, limitations and exclusions

The liability arrangements are key to entities' participation (both accredited and unaccredited) in the system, and it is vital that potential entrants understand all possible liability scenarios prior to making a decision to participate in it.

Section 79 of the draft Bill protects accredited entities from liability where the accredited entity "provides, or fails to provide, the accredited service in good faith, in compliance with this Act." An accredited entity that wishes to rely on this protection bears the evidentiary burden.

We support this approach. We also assume the protection from liability extends to the scenario where a fraudulent ID is used (by a malicious actor), assuming of course that the accredited entity has acted in good faith and complied with the legislation and rules of the system.

However, s 80 of the draft Bill does not limit liability for accredited entities in relation to non-compliance with the legislation and rules. While the Rules allow for provisions that could limit the kinds of losses and damages for which compensation could be sought and the amount of such compensation, the Rules as currently proposed do not include such provisions.

Bearing in mind that non-compliance is, in all likelihood, unintentional (accredited entities will not be deliberately setting out to avoid compliance with the Rules), an uncapped liability is

concerning and potentially a disincentive to participation for Communications Alliance members.

While we support the use of a statutory multiparty contract as the mechanism for accredited entities to be contracted to supply services to the system, we consider it does not address the concern of uncapped liability. The absence of any principles or rules to limit the liability through this contractual mechanism is concerning, especially where entities include Government agencies who are similarly eligible to recover loss or damages in the event of an incident.

Communications Alliance also notes that the Digital ID Regulator and the ACCC and their respective staff are to be excluded from liability (draft Bill, s 151).

Due to the high risk that any identity system will be a target for malicious actors, Communications Alliance suggests the following broad principles should be adopted for the creation of the Digital ID legislation and rules:

- The benefits of the framework will be shared by users, accredited entities, relying parties and by Government. Hence, the downside risks should also be shared, meaning all participants and Government should bear some liability.
- Accredited entities should not bear unlimited liability for loss and damage flowing from their non-compliances – liability for such losses and damage should be capped from the outset as part of the statutory contract.
- The Commonwealth should bear some liability for its participation in the framework. Its employees should not be immune from liability: they would be covered by the *Legal Services Directions*, which provide for the Commonwealth to give or fund legal assistance to an employee who has acted, or is alleged to have acted, negligently, i.e. failed to exercise the legal standard of 'reasonable care' owed in the circumstances, unless the employee's conduct involved serious or wilful misconduct or culpable negligence.

8. Digital ID Data Standards

We welcome the requirement of s 94 that Digital ID Data Standards be subject to a public consultation of at least 28 days.

To further ensure that industry can engage with the making of such standards, we strongly recommend that all Digital ID Rules be finalised prior to commencing the process of standards development.

Experience from the Consumer Data Right (CDR) standards development highlighted that our (and other) sector(s) had substantial difficulty to engage with the standards development process without knowledge of the exact requirements that were to be stipulated in the CDR rules. This led to difficulties to commit resources to such processes as well as substantial issues to adequately being able to assess standards proposals.

We also note that the commencement dates of the legislation and rules ought to provide for realistic timeframes for the (sequential) development of standards and subsequent implementation.

9. Decentralised approaches

The proposed framework appears to rest on the vision of a centralised model. However, the legislation and rules also ought to account for private and public sector innovation which could result in decentralised approaches. These ought not be excluded or impeded as long as they meet all relevant requirements contained in the legislation, rules and standards.

10. Conclusion

Communications Alliance appreciates the consultation that the Digital Transformation Agency and the Department have undertaken so far and looks forward to further engaging with the Department and all relevant stakeholders.

We reiterate our support for a national digital identity framework for Australia that will assist our nation in improving the privacy of personal information and the protection of identity information. The feedback provided seeks to further enhance the framework as envisaged by the legislation and rules.

For any questions relating to this submission please contact Christiane Gillespie-Jones on [redacted].

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507